The *ASK LEO!* Guide to

STAYING SAFE ON THE INTERNET

FREE EDITION!

6th Edition

askleo.com

LEO A. NOTENBOOM

The Ask Leo! Guide to Staying Safe on the Internet

Free Edition

6th Edition

by

Leo A. Notenboom

https://askleo.com

ISBN: 978-1-937018-69-6 (PDF)

6.0

Table of Contents

The Ask Leo! Manifesto

I believe personal technology is essential to humanity's future.

It has amazing potential to empower individuals,
but it can also frustrate and intimidate.

I want to give you more *confidence*.
I want to make technology work for you.

I want to replace that *frustration* and *intimidation*
with the *amazement* and *wonder* that I feel every day.

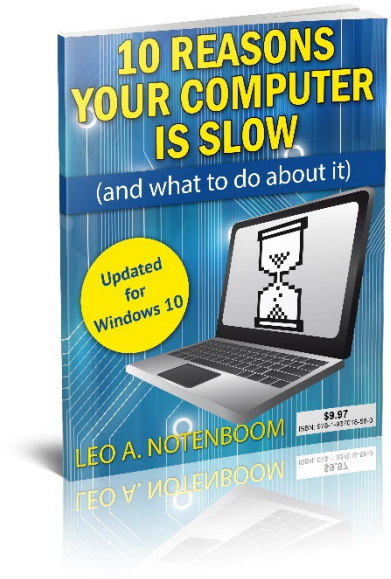
I want it to be a *resource* rather than a *roadblock*;
a *valuable tool,* instead of a source of *irritation*.

I want personal technology to empower you,
so you can be a part of that amazing future.

That's why *Ask Leo!* exists.

Leo A. Notenboom
https://askleo.com

First: A Freebie for You



You're looking at the free version of my Internet Safety ebook, and I hope it's useful to you.

But before we dive in, I have something more for you: my *Ask Leo!* special report, ***10 Reasons Your Computer is Slow (and what to do about it)***. This report will help you identify why your computer is slowing down, and the steps you can take to fix it.

It's yours free when you register *this* book.

In fact, you'll also several additional free bonuses.

- All available digital formats of the book as direct downloads. Regardless of which version you have, you can enjoy this book on the digital device of your choice.
- Digital updates for life.
- Errata and prioritized Q&A.

You'll find the information you need to register in a chapter near the end of the book. Once you register, you'll be taken to a webpage that lists all available bonuses.

Part 1: Protect Yourself

It Pays to Be Skeptical

A message pops up on your computer, warning you that malware has been detected.

What do you do?

The answer's not as clear as you might think.

In fact, no matter what you choose to do, it could be the wrong thing.

Your trust is a commodity

It's no secret that scammers actively prey on the trusting.

But it's not just scam artists who abuse our generally good nature and desire to trust. Hackers, malware authors, overly-aggressive salespeople—essentially anyone who wants something— re skilled at using your trust against your better interests.

Warning: malware detected, click to remove …

A pop-up message telling you there's malware on your machine[1] (and click here to fix it) is probably no big surprise to most people. With the constant barrage of news reports about hacks and malware and the ongoing emphasis on anti-malware tools,[2] your first response on reading such a message may be to believe it.

"Malware? Well, it happens to so many people, it's no surprise that it happened to me!"

Except … it might not have.

That message might be completely fake. It may be inciting you to trust it and click to take further action. And that click and "further action" could install malware, or worse.

Or it could be legitimate.

What do you do?

Unable to deliver package, details attached…

You've probably received an important-looking email telling you there's a package on its way and the details are in an attached file.[3]

[1] https://askleo.com/3107
[2] https://askleo.com/3517
[3] https://askleo.com/18718

Perhaps your online email provider has detected a problem with your account, and you need to check something by clicking on the conveniently provided link.[4]

I've even received email from "PayPal" indicating that access to my account had been "limited" because of suspicious activity. I needed to log in to provide additional information—once again, using the provided link.[5]

In each case, the sender wants you to trust them, and take whatever action they've recommended in their message, be it examining the contents of an attached file, clicking a provided link to their website, or even replying to the email with sensitive information.

Abusing your trust in this manner is currently one of the most effective ways to distribute malware or hack your online accounts.

And yet, each one of those scenarios could be legitimate at times.

What do you do?

I'm from Microsoft, and we've detected….

You're working on your computer one afternoon and get a phone call from someone who says they work for Microsoft. They've detected that your computer is causing many errors on the internet. They offer to walk you through some steps to show this to you, and indeed, there *do* seem to be lots of unexplained errors right there on your computer.

Then they offer to fix it for you,[6] if you'll just go to a site and type in a few numbers they recite to you.

Those errors are pretty scary looking, and you certainly don't understand them.

What do you do?

What you do: get skeptical

Skeptic: a person who has or shows doubt about something. – Merriam Webster[7]

If there were one skill I could magically impart to my *Ask Leo!* readers—hell, on the entire technology-using, internet-loving universe—it would be the skill of healthy skepticism.

I don't mean that you believe nothing and trust no one. I mean that you believe, you question, and before you trust, you learn.

Truly, being skeptical is really the only solution to the scenarios I've outlined above.

---

[4] https://askleo.com/132182
[5] I've actually received this scenario *legitimately*, which really surprised me. Of course, most are scams of some sort.
[6] https://askleo.com/4164
[7] https://www.merriam-webster.com/dictionary/skeptic

In each case, it's *critical* that you not blindly trust the information presented to you. In each case, you must question whether or not the person or company at the other end of the message has your best interests in mind. Is the story they're telling accurate? Verifiably accurate? Do you know beyond doubt that they are who they say they are?

> *"Skeptic: a person who has or shows doubt about something.*
> -Merriam Webster

If the answer to any of those questions is "no", or even "I'm not sure", *stop*. Stop and take additional steps make sense to confirm that what you're being told is legitimate.

It might mean some internet research, calling them back, or asking a trusted friend or resource for their opinion.

But if you aren't sure, question everything.

Be more skeptical: it's one skill that can help prevent disasters before they happen, and keep you and your technology safe.

Nullius in verba: "Take nobody's word for it."[8]

It's more than just technology

Naturally, my plea for being skeptical and that you "question everything" is about far more than just the technology you have sitting in front of you.

As I've written before,[9] an amazing amount of information we're shown each day is completely bogus—or at least nuanced and presented in such a way as to cause you to believe that things are other than they truly are.

Add to that our natural tendency to believe that which supports what we already believe (known as the "echo chamber" or "confirmation bias"), and it's exceptionally easy to be misled and misinformed.

The solution remains the same:

Be skeptical.

Question everything…

…even things you already believe are true.

[8] Nullius in verba, besides being the motto of The President, Council, and Fellows of the Royal Society of London for Improving Natural Knowledge, is a very fancy way of saying "question everything". ☺
[9] https://askleo.com/11287

Just What Is Common Sense?

When it comes to internet safety, one of the most oft-cited pieces of advice computer professionals hand out is:

Use common sense.

One of the most common responses is:

"Just what does that mean?"

When it comes to technology and safety, "common sense" is important, poorly defined, and quite *un*common.

Let's see if we can define it with some already-familiar rules.

Common sense can be summed up in several familiar adages:

- If it sounds too good to be true, it's probably not true.
- If it ain't broke, don't fix it.
- Free is never free.
- Read what's in front of you.
- Don't believe everything you read.
- Be skeptical: question everything.
- Do your research.

If it sounds too good to be true…

As we see so often, many malicious incursions mask themselves in promises of things that seem irresistible.

Practical examples of offers that really are too good to be true include:

- Many "free download" advertisements
- Software that promises to speed up your computer
- Ads that include the phrase "one stupid trick to…" or variants thereof
- Click-bait headlines that include the phrase "you won't believe" or "will blow your mind" or similar

Common to most of these items, beyond the fact that the promises they make seem extreme, is that *you weren't looking for them when you found them*.

Look at any website, and you'll see advertisements. Many are legit and well-positioned, but others are little more than over-the-top attempts to get you to click or download whatever they have to offer.

Particularly when you're not looking specifically for something, don't fall for extreme or outlandish claims. They are:

- All too common
- Very often completely false

The same can be said of most forwarded hoaxes and urban legends as well as many “news” stories on not-quite-reputable (or even satire) sites.

Common sense tells us if it promises too much, if it seems too extreme, if it seems too astonishing… then it’s probably completely false. Don’t waste your time.

If it ain’t broke, don’t fix it

Whether following over-inflated promises such as those I just mentioned or out of desperation, I often see people trying to do things to their computers that have nothing to do with a problem they’re experiencing.

- They try to solve speed problems they don’t have.
- They try to remove malware that isn’t present.
- They try to update software they don’t use.
- They try to fix problems that have nothing to do with their computer.

The list goes on.

I understand that each of those assumes a certain amount of knowledge. How do you know you don’t have a specific problem? How do you know malware isn't present? How do you know that the problem you’re experiencing is with the website you visit and has nothing to do with your computer?

That’s a fair concern. But if you don’t know you have a problem, why are you trying to fix it?

So turn the thinking around.

Common sense means not doing something because you might have a problem, but taking action because you know you have a problem and not before.

Research the problem first. Confirm you actually have a problem that needs fixing before you try to fix it.

(I’ll talk about research shortly.)

Free is never free

The economist’s old acronym is TANSTAAFL: “There ain’t no such thing as a free lunch.” That’s exceptionally true on the internet.

Every "free" service has a cost. It may be the advertising you see, the mailing list you need to sign up for, the personal information you're sharing, or something else entirely, but there is no such thing as “free” on the internet.

Most commonly, people fall into the "free" trap through advertisements of this variety: "FREE scan! Scan your computer for malware for FREE!"

Some of these ads are 100% accurate. The scan is completely free. The not-so-free part? If you want to do anything about what the scan finds, you'll need to pay. It's a common sales tactic.

Less reputable programs lie to you. They warn you of malware and other scary things you don't have or that aren't issues—all making it appear that giving them your money is the only way to avoid certain doom.

Which brings us to another important point.

Read what's in front of you

This is a point that frustrates me. It works like this:

- A program fails or something goes wrong.
- The user gets frustrated or confused.
- The user completely misses the fact that *the solution to the issue was included* in the error message or descriptive text.

Another similar scenario:

- Someone gets an email and reads the first line, which is so outrageous that their reactions kick in right there and they stop reading.
- As a result, they miss the text after that, which puts the statement in a clearer context or provides additional information and removes all the outrageousness.

When something goes wrong with your computer, take the time to read what's on the screen in front of you. I get so many questions that could be quickly dealt with had the questioner just slowed down and read the instructions in front of them.

I understand that those instructions are not always comprehensible. Honestly, I do. But sometimes they really are so clear and obvious that just taking the time to slow down and carefully read what's on your screen will get you a long, long way.

Which brings us to the flip side of the coin.

Don't believe everything you read

I'm a firm believer that people are basically good.[10]

But that doesn't mean that everyone is good or that everyone has your best interests in mind, particularly when it comes to the internet.

[10] That's one reason I took on heroicstories.org and run notallnewsisbad.com.

It's too easy, particularly in today's exceptionally connected and information-rich world, to spread misinformation as fact. We see it all the time.

Misleading ads are only one blatant example. Misleading ads pre-date the internet by decades, if not hundreds, of years. It's just that today's technology often makes it difficult to distinguish snake oil from valuable and effective medication unless we're careful.

The internet can also supply us with a wealth of information to help us separate over-inflated claims from reality.

It can also provide us with even more misinformation.

"It's on the internet, so it must be true" is one of those statements that everyone laughs at because it's so blatantly wrong, it's laughable. Common sense tells us that because something is on the internet has absolutely no bearing on its accuracy. Yet we see people act as if it is, believing random and misleading statements from vague sources with less-than-altruistic agendas.

With information coming at you from so many random directions from sources both reliable and unreliable, it's critical we do not believe everything we read just because it's been formatted attractively[11] on a site that looks authoritative.

And that brings us to the most important point of all.

Above all, be skeptical

Want something that's very common sensical?

Question everything. Even me.

Never accept information at face value, particularly on the internet, and particularly from sites or individuals you've never heard of before.

Be skeptical. Ask questions. Consider the source and what that source's agenda[12] might be in spreading its message.

Over time, develop a set of resources that you trust. Naturally, I hope *Ask Leo!* will be one of them, but honestly, what matters more is that you reach out and find sites, sources, services, and individuals that you trust.

Then use those resources to help you evaluate the constant stream of information and misinformation that's heading your way.

Yes, it's a little bit of work. But it's critical.

---

[11] Also not new. I'm fairly certain that my good grade on a paper I turned in while in college was due to the fact that I'd figured out how to use a word processor to make it look much better than it actually was.
[12] And don't kid yourself, every source has an agenda. More here: Stop spreading manure.

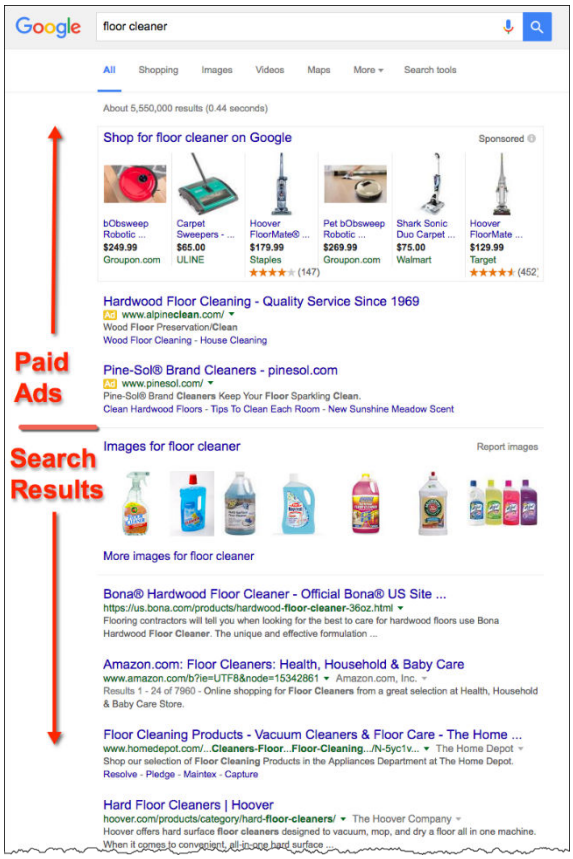
Do your research!

Search for yourself. Learn the basics[13] of how to not only use a good search engine (Google, Bing, or others), but also how to interpret the results. Understand the difference between advertisements presented on the search results page and the actual results (see image below).

Look for well-known, reputable sites you recognize in those results, not just sites that happen to rank highly. As much as the search engines work to make it not so, ranking highly in a search result is not an indication that the site is legitimate or trustworthy.

If you choose to look at information presented by a site you've never heard of before, remember, you've never heard of it before! Without more research, there's no way to know whether the information presented is valid, biased, or completely bogus.

Get help. If you're uncertain how to go about researching a particular topic, there's nothing wrong in asking for help. You may have more experienced friends or family members who can help you find what you're looking for. Librarians are also valuable resources when trying to determine the validity of information you run across online.



Regardless of who's helping you, it's still okay to be skeptical. When they suggest a site as a trustworthy resource, don't be afraid to ask them why they trust it.

Look carefully for confirmation. There are two types of confirmation:

- Source B repeating what source A has said.
- Source B independently presenting the similar information or conclusion that source A did.

The first isn't confirmation at all, it's repetition. The problem is, when enough sites and so-called sources all repeat what only one of them has said, it may feel like many sources have all come to the same conclusion. In reality, it's nothing more than a single opinion repeated over and over. This is known as the *echo chamber*.

Remember: repetition isn't confirmation. You want to find multiple sources that are confirming (or denying) the issue, and are doing so having arrived at their conclusions independently, using their own research.

[13] https://askleo.com/two-steps-better-search-results/

Use debunking sites. I'm a huge believer in using sites like snopes.com,[14] urbanlegends.about.com, factcheck.org, or any of several others before reacting to the latest over-the-top, can't-possibly-be-true news story, tech tip, or emailed rumor. Many are very timely and do the kind of research you want to see before getting all excited or worked up about what just landed in your inbox.

Use resource sites. There are resource sites for just about any topic. Develop a set of sites that you trust. For example, when it comes to technology, I would hope Ask Leo! is on your list. Visit the sites for which you already have a level of trust and see what they say about the issue at hand. As always, I'm not saying you need to trust them completely, but use them as part of your research to develop your own well-thought-out opinions.

The bottom line is this: if something you run across is worth the effort to take any action at all—even if it's just to forward an email—it's also worth researching first. At worst, it may save you some embarrassment. At best, it could protect your computer, your identity, and even your possessions.

[14] No, Snopes isn't left-wing biased. Generally people claiming so are simply unhappy with the truth Snopes has uncovered. Nonetheless, if you're not happy with Snopes, look at any of the multiple debunking sites that are available these days.

Stop Spreading Manure

Supposedly, in a report a few years ago, Google blatantly admitted that you should have no expectation of privacy whatsoever when using their services. The internet went crazy. Many sources seemed to say, "How outrageous! We told you so! Google is evil!" Mainstream news outlets picked up stories from smaller publishers, and they all seemed to confirm the entire sordid mess.

Except the internet was wrong. Manure, to use a polite term, was being spread far, wide, and fast.

This is where things get complicated.

Everyone has an agenda

In the popular television series *House*,[15] Dr. Gregory House often says, "Everyone lies."

On the internet, a similar statement can be made: everyone has an agenda.

Every website, news organization, and person sending an email, publishing a newsletter, or posting a comment has an agenda of some sort. They have something they want you to do, think, or become.[16]

All too often, the agenda being promoted is inconsistent (for lack of a better word) with reality.

The information presented is almost always colored by an agenda. People highlight facts supporting a particular agenda, conveniently minimizing or ignoring facts that don't. In the worst case, people fabricate facts to support their agenda.

Yes: not everyone, but some people, lie. Perhaps more often than you think.

To be honest, we all do it: we color what we say and do with data to support what we believe, often to the exclusion of all evidence pointing out the unthinkable: that we might be wrong.

If it's on the internet, it must be...

There's an interesting and somewhat strange conflict in our culture these days.

[15] http://www.imdb.com/title/tt0412142/

[16] My agenda is simple: I want you to be more skeptical before you believe what you see on the internet, and I want you to stop spreading misinformation. I'd love for this article to go viral and garner more Ask Leo! newsletter subscribers and site visitors, as well as improving my site's reputation with Google. I have a large agenda. And don't think for a moment that other sites, services, and individuals don't have agendas that are as large or larger.

Most people realize that "If it's on the internet, it must be true" is a sarcastic falsism expressing just how inaccurate information on the internet can be. *Just because it's published on a website somewhere (or shows up in your inbox, on Facebook, or wherever) doesn't make it true*.

However, I would wager that most people *do* believe most of what they read on the internet. Those same people smiling knowingly at that falsism go on to believe the strangest, most bizarre, completely false things as long as the information is presented in a seemingly credible way.

They do it without thinking and without seeing the irony in their behavior.

From what I've seen, this is getting worse.

We believe what we want to believe

A couple of terms help explain why this might be.

Confirmation bias is the natural tendency we all have to believe what confirms what we already believe and dismiss what doesn't. Confirmation bias can be as simple as dismissing alternative viewpoints out of hand and as horrific as being tried and arrested for expressing beliefs that are not commonly accepted (think Galileo[17]).

The problem with confirmation bias, as Galileo so clearly illustrates, is that it often stands in the way of the truth.

Put another way, we believe what we want to believe. We believe what matches our own world view and our own agenda *whether we are right or not*.

The *echo chamber* is the tendency of information sources—most notably news media—to repeat each other. In a sense, they use each other as sources. The problem is that a story originating from a single source—be it true or false—can appear to have massive objective confirmation when we start hearing that same story from a variety of supposedly independent sources.

Those sources aren't independent at all; they're just repeating what they heard from each other.

And it all started from a single source ...

... a source with an agenda.

Fifty shades of gray

Things get more complicated still.

[17] https://go.askleo.com/galileo

We desperately want things to be simple. We want things to be true or false, black or white, right or wrong.

Good or evil.

It's much easier to comprehend "true" and "false" than it is to deal with the potential uncertainty of "mostly true", "kind of wrong", or something in between. Unlike whether the sun circles the earth or the other way around, the issues that we consider, discuss, and even rant about are rarely so simple as to have easy, yes/no, black or white answers.

The folks who write headlines and push agendas know that thinking is hard for many of us. They know that black and white is easier, and (bonus!) much more sensational. So, they pick and choose the "facts" that support black-and-white thinking at the exclusion of the significantly more nuanced truth.

About that Google privacy thing

So is your email private with Google or not?

It's not that simple. It's still not a yes-or-no answer.

And yet:

- Organizations believed to have an anti-Google bias[18]
  - Drew a sensational black or white conclusion[19]
    - Based on a quote taken without complete and proper context[20]
      - Which was then bounced around the echo chamber on sites here,[21] here,[22] here,[23] and dozens of other media sites. [24]

Even though some sites posted clarifications and/or updates, they're often did so too late (the misinformation had spread) or too little (the clarifications remained biased to the pre-existing story or overall agenda).

Email privacy, and privacy on the internet in general, is a critically important and complex concept. Services like Gmail *do* process your email to do things like filter spam or populate indexes so you can search your email quickly. Are there teams of people sitting behind computer monitors reading your email? Almost certainly not.

---

[18] http://www.pcworld.com/article/204842/consumer_watchdog_fighting_google.html
[19] http://www.consumerwatchdog.org/newsrelease/google-tells-court-you-cannot-expect-privacy-when-sending-messages-gmail-people-who-care
[20] https://thenextweb.com/news/no-google-did-not-say-that-we-cant-expect-privacy-in-gmail
[21] http://techland.time.com/2013/08/14/google-says-gmail-users-have-no-legitimate-expectation-of-privacy/
[22] http://www.huffingtonpost.com/2013/08/13/gmail-privacy_n_3751971.html
[23] http://www.sfgate.com/technology/businessinsider/article/GOOGLE-If-You-Use-Gmail-You-Have-No-Legitimate-4730587.php
[24] These three were selected at random from an (irony alert) Google News search on "Google Privacy".

However, unless you encrypt your email, it is by definition fundamentally not secure. *This is nothing new* or specific to Google.

And yet, in the pursuit of clicks, page views, and furthering anti-Google sentiment, some sources pick and choose what to present, and then sensationalize how they present it.

You. Must. Think.

So what's the solution?

You. You are the solution. You and I and everyone we know must—and I really do mean *must*—become more skeptical and demanding of our news and information sources.

You and I must *think* about what we read. We need to learn to identify the sources and the agendas those sources have that color what they present and how they present it.

We need to learn to draw our own conclusions.

Whenever you accept misleading or inaccurate stories as truth, *you've been manipulated* to serve someone else's agenda. And when you pass those manipulative stories on to friends, family, and acquaintances? Well, my friend, you've just turned into a virtual manure spreader.

Because manure is what it is.

Be skeptical.[25]

If something sounds outrageous—*even if it supports your beliefs*—there's a hefty chance *it's completely bogus*. Overly sensational or outrageous-sounding headlines or content are a hallmark of bogus stories.

Do a little research. Check and verify the sources; follow the trail. If they all point back to a single source (or no source at all), realize what you're looking at. One source repeated a thousand times in a thousand places doesn't make it a thousand sources.

In the past, we could count on the media to do fact- and source-checking for us, but that's clearly no longer true. In the race for media outlets to publish quickly, the effort to make sure it's accurate has apparently been left behind.

Collateral damage: legitimate news and important issues

One of the truly sad casualties of all the misinformation on the internet is how difficult it has become to find the truth and how difficult it is for accurate, important news and information to get the attention it truly deserves.

It's all lost in the noise: covered in manure.

[25] https://askleo.com/21535

The non-profit world has a term: *donor fatigue*. This applies to potential contributors who, while supportive of a cause or organization, get tired of being asked for money, time, or whatever repeatedly.

The same is true here.

Call it *manure fatigue*. It is tempting to disregard anything found on the internet as likely to be bogus.

Unfortunately, there are legitimate outrages, atrocities, and issues of privacy[26] that really do deserve our attention, understanding, and even action.

It just takes some skepticism and some thought to separate the wheat from the fertilizer.

[26] https://askleo.com/21593

Why Ask Why?

I was helping a friend the other day with some Windows issues and a not-uncommon question came up, one that I often dread.

"Why?" As in, "Why did they do that?"

It's a common question that gets applied to computers and software of all generations and iterations. Recent versions of Windows have certainly generated a healthy share of "Why?" questions — but trust me, it's nothing new.

The problem is, asking "Why?" is an exercise in futility more often than not.

Don't ask out of frustration

Faced with something they don't understand, can't comprehend, or just don't like, many people ask "Why?" out of frustration.

Why were decisions made the way they were? What were they thinking? The questions may be mostly a way to emphasize just how much the questioner disagrees with those decisions. They're not really looking for an answer.

That's a good thing, because most of the time, there is no answer. Expecting one — in particular, one that would allow you to reconcile whatever issue you're facing and thus be OK with it — is just going to frustrate you when no answer is available.

Searching for a *why* out of frustration is energy wasted.

To get all Zen for a moment, it is what it is.

Getting frustrated, demanding to know why, or even understanding why isn't going to change any of that. You don't have to like it, but it's probably best to simply accept whatever it is for what it is and make decisions accordingly.

When the why isn't the real why

One of the most frustrating answers in technology when it comes to "Why?" is what I refer to as marketing-speak; you could even say misleading or misdirected marketing-speak, at that.

This happens when the source of our frustration believes we can't handle the truth, or simply doesn't want to share the truth, and gives us some corporate line about why a specific change was made.

A company might say they made a change because their tests revealed it was better, stronger, faster, or whatever, when in reality, the change was made to further some agenda. That agenda

might be about selling more product (not something they want to admit publicly), unifying some underlying technology (rarely a selling point), or laying a foundation for some future direction (that they can't yet admit to for competitive reasons). Or it could be some other random reason.

Whatever the reason, it's clear to those of us who use the resulting change that it's anything but better, stronger, faster, or whatever.

Once again, the reason doesn't matter. It is what it is. They did what they did for whatever reason they did it.

Live with it or seek out alternatives. In either case, move on.

Often, the answer doesn't help

Sometimes, you get lucky and actually find out why something is the way it is. And once you know why… you're no better off.

"Why did they change the user interface?"

"So it would be consistent across all kinds of devices."

"But I don't use other devices. Besides, it doesn't work on the device I do have."

Doesn't matter. That's what they did and that's why they did it. Maybe it makes other people happy. Maybe someday it'll make you happy when you get another device. Maybe it'll never make you happy. Doesn't matter. It is what it is.

Sometimes understanding why just doesn't help.

Do ask "Why?" out of curiosity

I don't want to make it seem like you should never ask why. "Why?" is an important question when you're curious. When you're trying to learn how things work, the question "Why?" is often an important step to understanding something in order to make better use of it.

A genuine "Why?" often uncovers rationales that can help you make sense of how things are connected and how things relate.

When you ask "Why?" in an attempt to learn something, it may occasionally be out of momentary frustration, but you're genuinely interested in the answer.

On the other hand, asking "Why?" out of pure frustration because you encounter something you don't like is rarely an educational or helpful experience.

Part 2. Protect Your Data

Why Is "Back Up First" Your Recommendation for Everything?

> *"In your response to the Spectre and Meltdown vulnerabilities, the first thing you recommended was to back up. Why? How does that relate to anything? How does backing up help protect me from malware and vulnerabilities?*

I harp on backing up a lot, I know. But it's on purpose.

As I've said elsewhere, nothing protects you and your data like a complete, recent backup.

Why back up first?

A complete system image backup taken prior to a change, update, or malware's arrival represents a safety net. If anything goes wrong, restoring that backup returns your computer to the state it was in prior to whatever it was that happened.

The backup I'm talking about

I want to be clear that the kind of backup I advocate is a *complete system image backup*. That's a backup of your entire hard disk, including your operating system, installed programs, any hidden partitions, and your data.

Other types of backups are certainly better than nothing, and it's incredibly important to back up at least your data, but for the kinds of issues we're about to consider, it's a system image backup that will save your bacon.

Vulnerabilities make you vulnerable

Once vulnerabilities are discovered in software, if malware gets on your machine, it now has a known way to exploit that vulnerability and wreak havoc.

Depending on the specifics, you may or may not be able to remove the malware through traditional means — for example, by using an anti-malware tool. Even then, once your security software says the malicious software has been removed, there's still no way to know with 100% accuracy it's correct. Malware's #1 job is to hide, and there's really no way to know your security software saw through all possible deceptions.

Short of reinstalling your system from scratch, *restoring from an image backup taken prior to malware's arrival is the only way to know for sure the malware has been removed*.

So, whenever I hear the phrase *new vulnerability discovered*, I immediately think "Back up!" — and use that as an opportunity to remind everyone of what I've just described.

Read-only vulnerabilities are gateways to more

Here's one way a backup can rescue you.

Some vulnerabilities only enable reading of protected memory areas. All they do is read data, so they can't damage anything, and you won't lose any data — right?

Consider the following scenario:

- Malware infects your machine.
- That malware uses some vulnerability to read otherwise protected operating system internal memory.
- What that malware finds is information that allows it to request and be granted administrative privileges on your computer.[27]
- With administrative privileges, the malware can read, write, encrypt, delete, or destroy whatever it has a mind to.

The vulnerabilities don't directly harm you; they enable the malware's ability to harm you.

Again, a backup protects you from the majority of that harm.

Updates can cause problems

Another scenario in which backup will save your bacon can occur around Microsoft updates. What's frustrating to everyone involved is that Microsoft's track record of providing stable updates is sometimes questionable. A few users find themselves in this unenviable situation:

It's important you take all updates to protect yourself from malware that might exploit the vulnerabilities.

- The update you take might "brick" your machine.
- Point #2 should never happen—and it doesn't happen often—but it can.

A complete system image backup taken prior to the update will protect you from the update if the update goes bad. If you find your machine unresponsive after the update, you can restore the backup image and wait for the update to be … updated … so it's no longer problematic.

Yes, absolutely, it's extremely frustrating if this happens to you. But *it's important not to let the fear of updates prevent you from updating*. A complete system image backup is your fear-reducing safety net.

It can't get any worse than this

An image backup represents a snapshot of your entire computer at a point in time — a snapshot you can revert to should anything untoward happen.

When you can always revert to that snapshot of your machine, *no matter what happens from that point forward, it can't get any worse*. If it does, you revert.

[27] While the operating system wouldn't keep the administrator password lying around in easy-to-read plain text, we can probably assume that malware poking around in the operating system's protected memory could find something it could use to this end.

That's why any time I'm faced with risk, I back up. Be it installing major updates, performing clean-up and/or repair operations, replacing or upgrading hardware, or just making changes to the work you keep on your machine, a backup is your safety net.

Do this

Back up.

Back up often.

Sooner or later, you'll be very, very glad you did.

And it'll always be part of my response. :-)

How Do I Back Up My Computer?

> *"How do I "back up" my computer? I am sure my question is ridiculous to you, but I honestly have no clue what I should be doing.*

Your question isn't ridiculous at all. In fact, I'm certain it's one reason so many people don't back up: they simply don't know how.

For something as critically important as backing up, that's more than a little scary. I hear from people who've lost important and valuable information all the time. Whether it's from malware, hardware failure, account hacks, or other disasters, a backup could easily prevent such loss.

First, let's look at what it means to back up a computer and what your options are. Then, I'll share some guidelines and tell you what I recommend for typical users.

Backing up

To back something up is to make a *copy* of it, and then keep that copy in a safe place.

That's it.

The key word in that statement is *copy*, as in duplicating the information. After you back up, you have the same information in two or more places.

That leads to my most important rule:

If it's in only one place, it's not backed up.

Folks occasionally misunderstand the concept. After copying their information to their "backup" drive, they delete the original. That means there's still only one copy: the one on that backup drive. Regardless of what you call the drive it's on, *if it's in only one place,* it's not backed up.

The purpose of a backup is simple: if something happens and you can't get your information from your computer or online account (which happens much more often than you probably realize), then you get the data from the backed-up copies—you haven't lost it forever.

So the concept is simple. Backing up starts to seem complicated when you look at all the options related to how much to back up, how often, and what tools to use to make sure it happens regularly.

Types of backups

Backing up generally takes one of two forms.

- Copying your data. If you copy pictures from your digital camera to your computer without deleting them from the camera, that's a backup. If you then burn those pictures to a DVD for

safekeeping, you've backed them up again. Similarly, if you take the contents of your "My Documents" folder tree and copy it to another machine or burn it to DVD, you've backed those files up.
- Imaging your system. Rather than backing up this and that, hoping you're including everything that might be important, a full-image backup copies *absolutely everything* your data, your programs, your settings, and even the computer's operating system itself.

Both types of backups share two important characteristics:
1. The backup creates a *copy* of the data.
2. That copy is placed *somewhere else*.

If your data is in only one place, meaning that there are *no copies* of that data, then you're not backed up.

Backup locations

So where should this "somewhere else" be?

Well, the ideal answer is "as far away from your computer as practical."

The further your backup lives from the original, the more types of disasters you'll be protected from.
- If the backup is on the same hard disk, and that hard disk dies, you could lose your data *and your backup*.
- If the backup is on a different hard disk inside the same computer, and something happens to the computer that causes both hard disks to be harmed (like a power supply failure), you could lose your data *and your backup*.
- If the backup is on an external hard disk but connected to the same computer, and there's a software glitch or malware on that computer that starts destroying files on all connected devices, you could lose your data *and your backup*.
- If the backup is on a different computer on the same network, a network problem or malware on your local network could start deleting files, including your data *and your backup*.
- If the backup is copied to a DVD, USB stick, or external drive and kept in the same *physical* location, and that location suffers a physical catastrophe such as a fire or flood, you could lose your data *and your backup*.

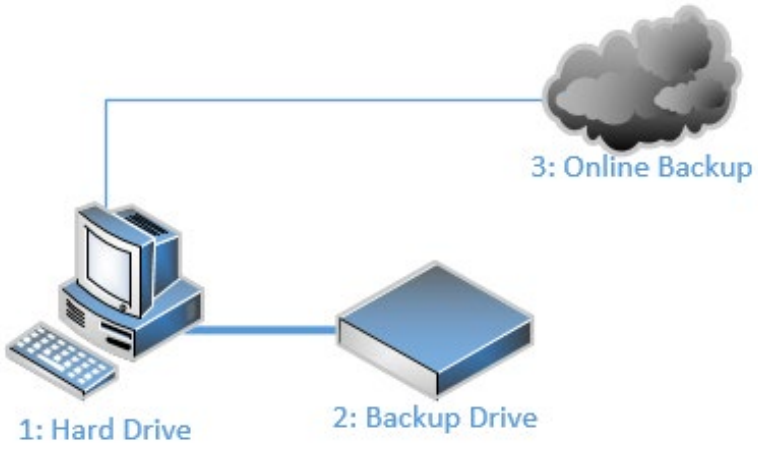
The closer your backup is to the original, the greater the possibility you could lose both at once.

It doesn't happen often, but it can.

Backing up in 3, 2, 1...

A great overall strategy for backing up is what many refer to as the "3, 2, 1" approach.
- 3 copies
- 2 different formats

- 1 copy kept off-site



Three copies

If a backup is "a" copy, why are we suddenly talking about *three* copies?

Because stuff happens. Backups fail, and if you believe in fate (or Finagle's law[28]), they'll fail just when you need them most.

If for no other reason, consider this scenario:

- You have a (single) copy of your data as a backup. Good for you. :-)
- Your hard disk dies and all data on it is lost. But you have your backup!
- But now you have *only* your backup—a single copy of your data.

Without your original hard disk, your data is in only one place. Until you make another copy, *it's not backed up...*

... unless you had your data in three places. Then you could lose any single copy and still be backed up.

Two formats

Every possible backup approach carries some risk of failure. Nothing is ever perfect.

For example, CDs and DVDs, USB sticks, external drives, and on-line backups are all subject to different types of risks of failure.

Using more than one type of backup is all about reducing the risk of a backup not being there when you need it.

[28] https://go.askleo.com/finagle

One off-site

As we saw earlier, the further your backup copy is from the original, the more you're protected. In particular, many people overlook the risk of theft or physical disasters (such as fire) to the data they have in their home or business.

Storing critical data somewhere else—somewhere else *physically* —means that no matter what happens to your computer or the backups you're creating onsite, you'll always be able to recover the information kept elsewhere.

But how do I do all that?

Even with these guidelines, the original question remains: just *how* should you back up?

The questions that drive your answer are:

- How likely is it that something will happen to your data?
- How important is your data?

From my experience, I will say that the answers tend to be:

- More likely than you think.
- More important than you think.

The three most data-loss scenarios I see people go through are:

- Malware
- Hard drive failure
- Accidental deletion

Without fail, they're surprised that it happened to them. What happens next depends on how well they prepared.

Protecting yourself against at least those three scenarios is a great place to start.

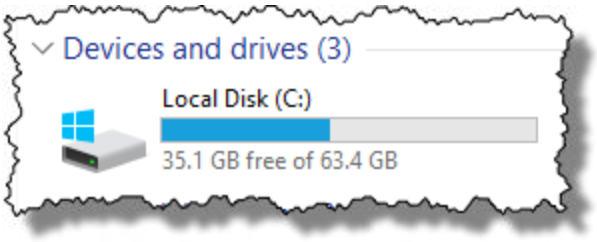
A 1, 2, 3 suggested backup plan

There are many approaches to backing up. Rather than trying to cover them all, I'll make a simple suggestion that will work well for most people.

1. Get an external USB hard disk

The first question that probably comes to mind is "how big?" There's no blanket answer, but I'll throw out this guideline.

Examine your computer's hard drive using Windows Explorer and determine how much data is on the drive.



If your 64-gigabyte hard drive has 35 gigabytes free, that means that you have 29 gigabytes of data stored on that drive.

Get a hard disk at least four times bigger. Using my example, I'd get (29 times 4) at least 116GB.

As I write this, it would actually be difficult to get a drive that *small*, given that drives are now more commonly measured in terabytes, or 1000 gigabytes. Your numbers will vary, of course, but when in doubt, go big; there's no such thing as a drive that's "too big".

2. Get backup software

I strongly recommend using a dedicated, automated backup program like Macrium Reflect,[29] EaseUS Todo,[30] or an equivalent to create image backups on your external drive automatically on a daily or weekly schedule. (You can use the backup software included in Windows, but to be honest, I find these dedicated tools to be more reliable, more flexible, and, most importantly, more transparent in their operations.)

3. Backup data online

Use a service like Microsoft OneDrive, Dropbox, or others to automatically backup your most important data, including the files and folders you're working on day-to-day.

These tools are primarily data-sharing tools; their primary purpose is to replicate your data across multiple machines, as well as on their own web-based interfaces. Because they make your files available online, these services copy your data to their servers.

In other words, it's an easy and often nearly-instant "somewhere else" to back up your data.

Now, to be clear, this recommendation won't protect you from absolutely *everything*, but it will protect you from a lot. In fact, it'll save you from what I see almost every day as the most common causes of data loss.

If your hard disk dies, you can restore files (and perhaps the entire system) from your backup. If you happen to—oops!—delete a file by accident, as long as it was there when the most recent backup was taken, you can restore it quickly and easily. If malware strikes, you can restore your system from a backup taken prior to the infection.

---

[29] https://askleo.com/4996
[30] https://go.askleo.com/todofree

Most programs come with relatively simple instructions to set up the most common types of backups for average users.

Starting with the 1, 2, 3 approach provides you a good base. If the importance of your data requires stronger measures, you can build from there.

How to Back Up Windows 10 or 11

You may have heard I'm a huge fan of backing up.

Microsoft Windows includes several tools that, used together, provide a backup strategy protecting you from almost anything **that can go** wrong.

Let's review what it means to use those tools together properly and get you backed up. We'll also review the impact of Microsoft's decision to phase out one of those tools.

We'll look at eight basic steps and four additional tips that acknowledge Microsoft's plans to phase out one of the tools.

1. Make an image

Start by making an image backup of your computer. It doesn't matter if you don't know what to do with it; that'll come later. Creating an image of your computer gives you a known point to which you can always return should anything go wrong in the future.

Creating a Backup Image Using Windows' Built-in Backup[31] walks through the steps to create a complete image backup of your machine on an external hard drive using what Windows 10 calls the "Windows 7" backup and restore tool.

2. Make a recovery disk

Next, I recommend you make a Windows recovery drive. This is a disk (a DVD or USB thumb drive) from which you would boot your machine in order to restore the image you created in the first step. The Windows recovery disk includes additional tools to examine and possibly repair your system, as well as the ability to reinstall Windows from scratch if needed.

Create a Windows Recovery Drive[32] illustrates the process of creating a recovery drive. You may also want to review the article How Do I Boot from CD/DVD/USB in Windows 8 & 10?[33] (which also applies to 11) and test to make sure you can boot successfully from the recovery drive you've created.

3. Restoring an image

Restoring an image is the process of taking a backup image you've previously created and putting it back on your computer's hard drive (which erases anything currently on that hard drive). An image restore is what you would do after replacing a faulty hard drive with a new, empty one.

[31] https://askleo.com/28186
[32] https://askleo.com/28233
[33] https://askleo.com/5356

Restoring an Image Backup Using Windows Built-In Backup[34] uses the image we took in step 1 and the recovery drive created in step 2 to demonstrate the process of restoring that image to your computer.

4. Restoring files from an image

I rely on image backups primarily because there's no question about what's in them: everything. But sometimes you don't want to restore everything; you just want a single file, folder, or collection. Microsoft doesn't make it obvious, but you can do that from a backup image you create using the Windows backup tool.

Restore Individual Files from a Windows Image Backup[35] shows you how.

5. Set up File History

In addition to image backups, we can utilize more "in the background" backups in the form of File History. File History sets aside some amount of space on your hard disk (ideally an external hard disk, and possibly the same one containing your backup images) to which it writes copies of your data files each time they change. Using File History, you can recover a file as it was an hour ago, a week ago, or sometime in between, depending on how often files change and how much space you've set aside for backups.

Enable File History in Windows[36] tells you how to set it all up.

6. Restore a file using File History

After you've had File History running for a while, you'll surely encounter a point where you want to recover a file that has been backed up.

Learn to browse what's been backed up, locate the file or files you want, and restore them in Restoring Files with File History.[37]

7. Use OneDrive for backing up

Backing up to a completely different physical location — "offsite" backup — has never been easier since the advent of cloud storage and synchronization tools like OneDrive.

Using OneDrive for Nearly Continuous Backup[38] not only shows you how to set up and configure OneDrive itself, but also discusses a couple of simple changes to your workflow that result in almost continuous cloud backup of all your work in progress.

[34] https://askleo.com/28416
[35] https://askleo.com/28536
[36] https://askleo.com/28383
[37] https://askleo.com/29116
[38] https://askleo.com/29368

8. Restore a file from OneDrive history

Just like File History, the day will come when you need to recover a file that's been backed up to the cloud.

Recover Deleted Files in OneDrive[39] points out that OneDrive has a Recycle Bin from which you can recover deleted files. As a bonus, Recovering from Ransomware with an Online Backup[40] discusses how it can even save you from ransomware.

But change is coming, so…

Used together, these eight steps and three tools (image backups, File History, and OneDrive) can provide an adequate level of backup for the average user. Best of all, you already have them in Windows.

For now.

Apparently, as of some time in 2020 (or even earlier) Microsoft decided to pull the plug on the "Windows 7 Backup and Restore" tool. At the least, it has been "deprecated" and will likely be removed in a future Windows update. The official word from Microsoft is that you should use third-party utilities instead.

The following bonus four steps do exactly that: show you how to perform steps 1 through 4 above using the free edition of EaseUS Todo instead of Windows 7 Backup and Restore.

9. Make an image using EaseUS Todo

Creating a Backup Image Using EaseUS Todo Free[41] illustrates how to create an image backup of your system to your external hard disk.

10. Make a recovery disk for EaseUS Todo

Creating an EaseUS Todo Emergency Disk[42] displays the process of creating a recovery disk — what EaseUS calls an "emergency disk" — that can be used to restore an EaseUS Todo image. It won't have the additional tools the Windows recovery disk created in Step 2 had, so you may want both, but you'll need an EaseUS emergency disk to be able to restore images created by EaseUS Todo.

11. Restore an image using EaseUS Todo

Restoring an Image Using EaseUS Todo[43] tells how to restore a backup image created by EaseUS Todo to your hard disk, replacing everything on it.

[39] https://askleo.com/29457
[40] https://askleo.com/29736
[41] https://askleo.com/29600
[42] https://askleo.com/29683
[43] https://askleo.com/29825

12. Restore an individual file from an image using EaseUS Todo

Restoring a File from an EaseUS Todo Image Backup.[44] EaseUS Todo makes restoring individual files and folders from an image backup easy.

Backing up is important. I say it so often because it's so true.

I also say it because I see so much data loss and accompanying heartbreak when people don't realize just how important it is until it's too late.

Use the steps above to make sure you're appropriately backed up and never suffer data loss again.

[44] https://askleo.com/29849

Part 3: Protect Your Computer

Eight Steps to a Secure Router

> *"I'd like to know how to clear the history of my Linksys router. I'd also like to know how I can make it more secure and protect it from hacking.*

The topic is an important one: how do you make sure you have a secure router? It's your first line of defense against automated malware attacks trying to get at your computer from the internet to install more malware.

You want to be sure there aren't any big gaping holes. Very often and by default, there are.

Here are the most important steps to a more secure router.

My router versus your router

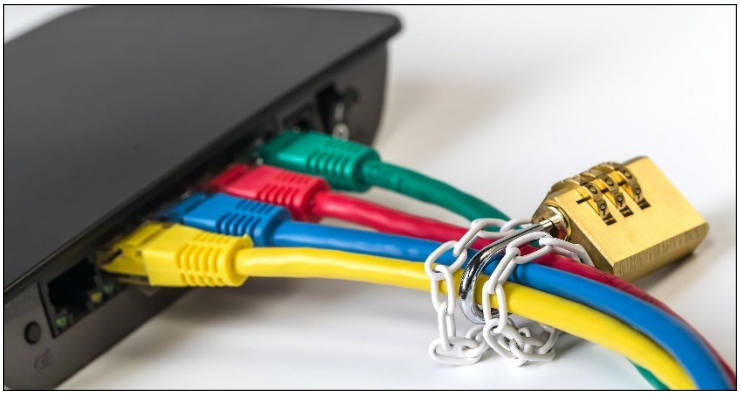
I have to start with a caveat: there are hundreds, if not thousands, of different routers. Different brands and different models with differing capabilities, power, and, of course, at differing cost.

Most importantly, they have different administration interfaces.

What that means is, I can't tell you exactly how to make changes to your router step-by-step. The concepts I'll cover apply to almost all consumer-grade routers, and I'll be using an old and popular LinkSys BEFSR81 router and LinkSys WAP54G access point as examples.

You'll need to "translate" the examples to the equivalent settings on your own router or access point. Make sure you have access to the documentation that came with your router, or locate the user's manual online.

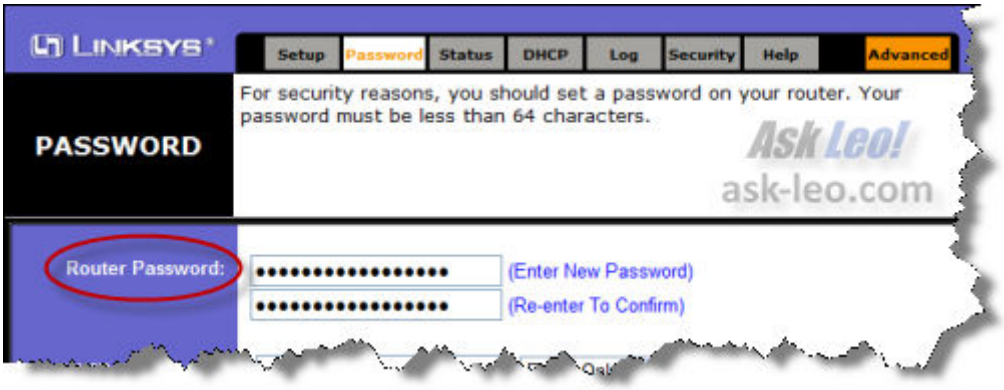
Already we see a common difference: you may well have a single device that combines both the router and wireless access point. You probably refer to it as simply your "router". In reality, there are two separate devices—a router that deals with network access, and a wireless access point that provides your Wi-Fi connectivity—that happen to be housed in a single box. In my case, they're in separate boxes.



1. Change the default password

If you do nothing else to secure your router, *change the default password*. Change it to be something long and strong.[45] If your router supports it, a pass*phrase* of three or more words might be ideal.

[45] https://askleo.com/4844



The reason for this is quite simple: it's a common gaping security hole.

For many years, almost every router and access point from the same manufacturer was shipped with the same default password. For LinkSys, if your login is a blank username and a password of "admin", as outlined in its manual, then *anyone and everyone knows it.* And anyone can log in to your router and undo any or all of the rest of the security steps we're about to take.

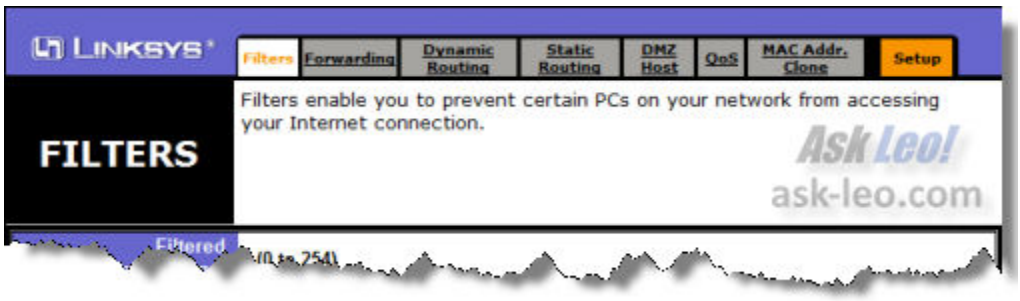
Then, any malware that takes advantage of the default passwords on routers can make changes without your knowledge.

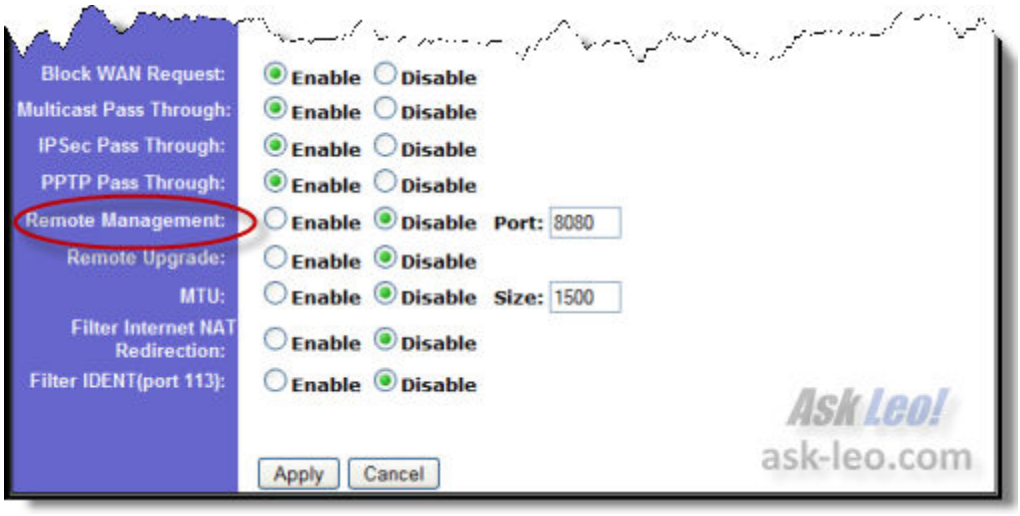
Fortunately, in recent years, most—though not all—router manufacturers have been getting smarter. If the instructions that came with your router included checking a sticker on the actual router for the admin password, and that looks like a strong password, then the security hole is significantly smaller. Now only those people who can walk up to your router and look at that sticker can get in.

I'd change the password anyway.

2. Disable remote management

"Remote Management" is a feature that allows your router to be administered from anywhere out on the internet.





While this setting (coupled with a *very* strong password) might make sense for a handful of people,[46] for most folks there's absolutely no need to administer the router from anywhere but the local machines connected to it.

Make sure the remote management setting is off.

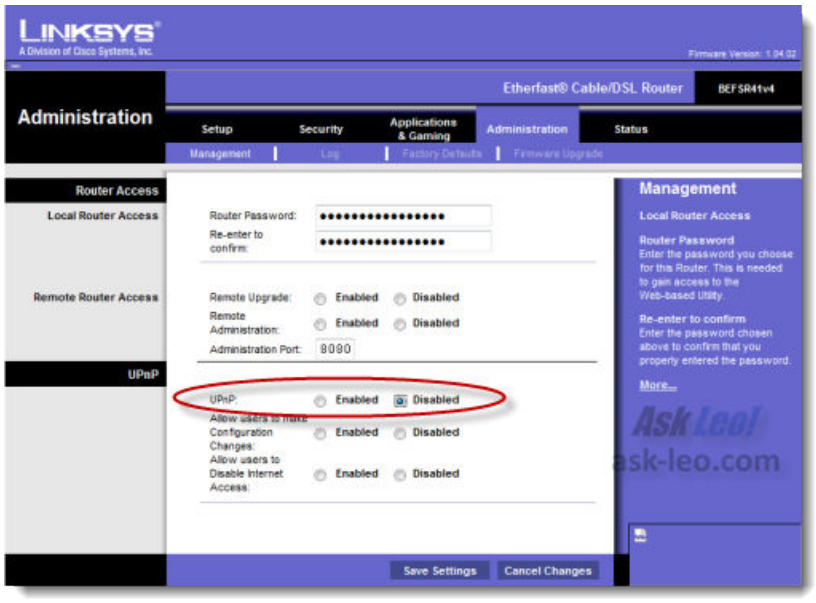
3. Turn off Universal Plug and Play

Universal Plug and Play (UPnP) is a technology that allows software running on your machine to configure services like port forwarding (a way of allowing computers outside your network to access your local computers directly) without you having to go in and administer the router manually.

It seems like a good idea, right?

Nope. Turn it off.

[46] Some ISPs will insist on this, but they'll also prevent you from administering your own router as well. More common is a scenario where you're responsible for supporting someone else's network – say that of a friend or family. Remote administration can be helpful in a case like that. Even so, I'd think twice about setting it up, and would insist on an exceptionally secure password if you do.

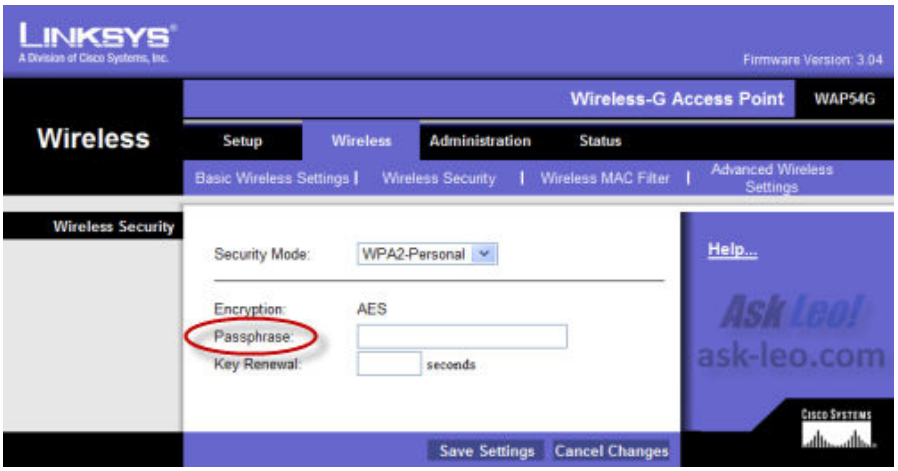


It turns out that malware can also be UPnP aware, and can make malicious changes to your router without your involvement or awareness.

(Note: UPnP is *unrelated* to Windows "Plug and Play" hardware detection; it's just another unfortunate collision of similar names.)

4. Add a WPA2 key

It's time for another password, this time to secure and encrypt your wireless connection.



First, use **WPA2**, *not* WEP. WEP encryption turns out to be very easily crackable,[47] and even WPA (without the 2) has been shown to be vulnerable.

[47] It's essentially like having no encryption at all.

Second, just as you did for the router's administration password, select another good, secure key/password/passphrase (the terms are roughly interchangeable here). You only need to enter it once here and once on each machine allowed to connect to your wireless network.

Having a strong WPA2 key ensures that only machines you allow on your network can see your network, your traffic, and your router.

5. Disable WPS

WPS, or Wi-Fi Protected Setup, doesn't live up to its name—it's not very "protected" at all.

WPS was intended as a way to make setting up a protected Wi-Fi network easy. WPS would, with the push of a button, set up Wi-Fi encryption between the router and clients that supported it.

The problem with WPS is that the protocol is flawed in such a way that it is vulnerable to a brute force attack. A malicious entity within range can force their way onto your network, bypassing any encryption keys you might have set up.

WPS is enabled by default on many routers. Turn it off.

6. Turn off logging

This has less to do with configuring a secure router, and more to do with maintaining your privacy.

This is also about making sure logging is still turned off, since if a router supports any kind of logging at all, it'll likely be off by default.

Disable the logging, and no information will be kept on the router, or sent to any other machine. This should also clear any log the router has.

It's worth pointing out that most consumer-grade routers do not have the capacity to actually keep complete logs themselves. If they keep anything, it will only be a shorter, partial log. When enabled, some will offer to send the log to one of the computers on your network for storage. Simply disabling logging will not erase any logs stored elsewhere.

7. Secure your router physically

As we've already seen, even if the default administrative password is unique to your device, it's still visible to anyone with physical access to the router who can see the sticker on which it's printed.

In fact, your secure router may not be secure at all if anyone can just walk up to it.

All of your router's security settings can be reset in a flash if someone has physical access to the device. Almost all routers have a "reset to factory defaults" mechanism (typically by holding a reset button for a certain amount of time). If someone can walk up to your router and do that, all the security settings you've just enabled may be instantly erased.

Only you can judge whether or not you need this extra level of physical security, but make sure to consider it. It might be as simple as keeping the device in a locked room or closet.

8. Check for firmware updates

Routers (and access points) are really just small computers dedicated to a single task: handling network traffic. Normally the software — referred to as “firmware” since it’s stored within the device’s hardware — is solid and just works.

Unfortunately, security vulnerabilities are sometimes discovered, requiring you to update your router’s firmware to stay secure. This usually involves downloading a file for your specific router and using its administration interface to install the update. Some routers can fetch and install the update directly. Either way, the update is a manual step you need to take.

Checking to see if there’s a firmware update for your router is also a manual step. Some routers perform the check at the push of a button in the administration interface. If not, you need to visit the manufacturer’s support site, look for information pertaining to your specific model, and determine if a newer version of the firmware is available.

Two steps that aren't steps

Each time I mention this article, folks make two additional suggestions for Wi-Fi specifically that, do not improve security at all. In fact, they may harm security in some ways by providing a false sense of added security.

The first is MAC address filtering. I discuss this in more detail in Is MAC Address Filtering a Viable Wireless Security Option?,[48] but the bottom line is that like a cheap padlock, MAC address filtering only keeps out honest people. If someone wants to access your network MAC address filtering is easily bypassed.

The second suggestions is to turn off SSID broadcast on wireless networks. Even when not being broadcast, the SSID is still visible—unencrypted—in the packets of traffic sent to and from the router. Disabling the broadcast, does nothing to prevent someone with the skills from easily

[48] https://askleo.com/4350

discovering it. I discuss this in more detail in Does Changing or Disabling the Broadcast of My Wireless SSID Make Me More Secure?[49]

When it comes to Wi-Fi, putting a WPA2 password on the connection is currently your best security measure.

[49] https://askleo.com/5049

What Security Software Do You Recommend?

> *"What security software should I use? What anti-virus is the best? How about a firewall? And what about spyware? Should I use one of the all-in-one packages that claim to do everything? Is there anything else I need?*

As you might imagine, I get questions like this all the time. As a result, I do have recommendations for security software and techniques to stay safe in various articles all over *Ask Leo!*

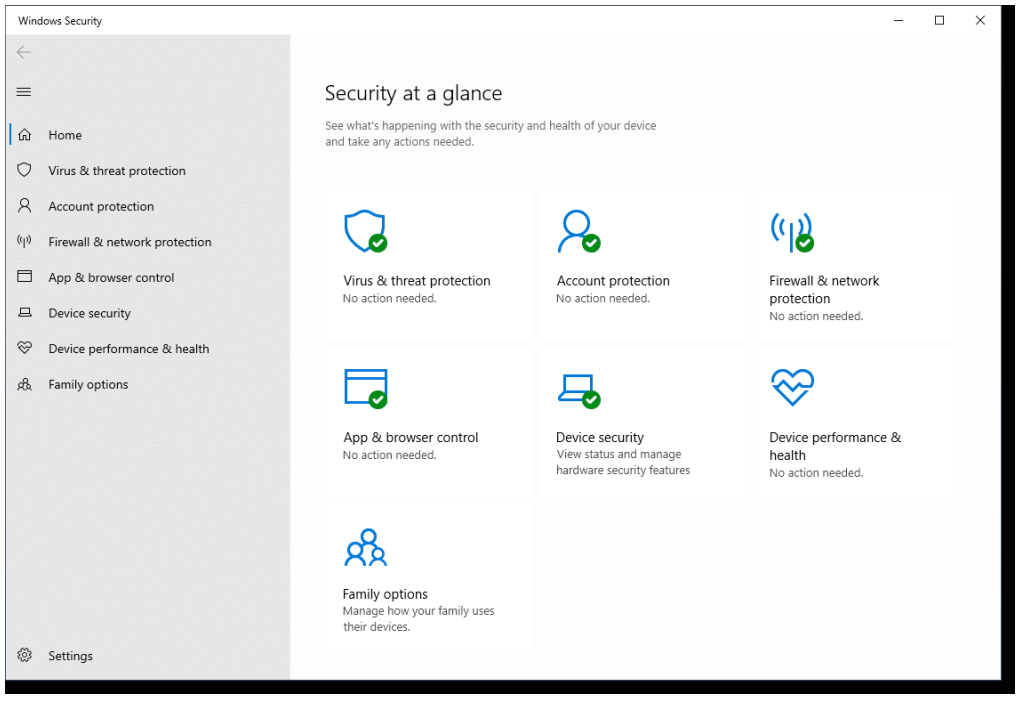
To make your life a little easier, here's a short version that sums it all up into four steps.

The short-short version

- Windows 10 and 11's Windows Security is my recommended anti-malware tool for most.
- Your router can serve as your primary firewall at home or work.
- Leave the Windows firewall enabled as well, unless it causes problems.
- Let Windows Update keep your computer as up to date as possible.

That's it. Good basic protection in four steps. That's it.

Basic security software: Windows Security



In Windows 10, Windows Security -- previously known as Windows Defender -- comes pre-installed. Microsoft seems to be improving it with every release.

Windows Security does a fine job of detecting malware without adversely impacting system performance or nagging you for renewals, upgrades, or up-sells. It just does its job quietly in the background -- exactly what you want from your anti-malware tool.

The ratings game

Every so often, Windows Security comes under fire for rating lower in tests published online than other security packages. I get push-back -- often angry push-back -- that it remains my primary recommendation.

There are several reasons I stick to that position.

- No anti-malware tool will stop all malware. Malware can and does slip by even today's highest-rated packages.
- "Highest-rated" changes depending on the date, the test, and who's doing the testing. There is no single clear, consistent winner.
- Regardless of how the data is presented, the differences among detection rates across most current anti-malware tools is relatively small compared to other factors.

There are also some practical reasons I continue to prefer Windows Security.

- It's free.
- It's already installed; there's nothing you need to do.
- It rarely impacts system performance.
- It keeps itself up to date using Windows Update.
- It has no hidden agenda -- it's not going to pester you with renewals, upgrades, or up-sells to tools you don't need.

It's not perfect, but no security tool is.

My recommendation stands. Windows Security remains a solid, free security package with minimal system impact. It should be appropriate for almost everyone.

Alternative security software and additions

I also recognize that Windows Security might not be the right solution for everyone. No single product is.

This is where I run into some difficulty trying to make recommendations. The landscape keeps changing. Tools that were once clearly free have, on more than one occasion, moved to promoting their paid product so heavily that the free version virtually disappears. People download and install programs thinking they are free, only to discover it's a "free trial" or "free download" (if you want to keep it past a certain length of time, you're required to purchase it).

Some programs have become as much self-promotion tools as they are security tools, bombarding you with sales pitches and upgrade offers to the point of getting in the way of your work.

Things keep changing. So to the extent that I mention specific tools below, *caveat emptor*: "Let the buyer beware." I can't honestly predict that the tools will remain recommendation-worthy.

Malwarebytes Anti-Malware[50] has evolved over the years into a full-featured security package. It continues to have a good track record for removing troublesome malware other packages sometimes miss. (And yes, there remains a free version: after the "trial" of their pro version ends, what remains is the free version. The free version is an on-demand scanner only.)

AVG,[51] **Avira**,[52] and ~~Avast~~,[53] or the "three AV's", as I like to call them, are three other free solutions I've recommended over the years. I continue to hear good things and not-so-good things about each, often in waves as each make significant updates.

Other name-brand (but potentially not free) solutions include Kaspersky,[54] McAfee,[55] WebRoot,[56] and BitDefender.[57] [58]

Caveats with all

I need to reiterate some important points.

- Beware of "free". In most cases, a "free trial" is just that: a trial of a full-featured product eventually requiring payment. In some cases, like MalwareBytes, the "free trial" becomes a truly free version after the trial ends. In other cases, they are two separate downloads. And in other cases, there is no truly free version at all. Be sure you know which you are getting.
- Regardless of which you download, you are still likely to be faced with upgrade and up-sell offers, or even an ongoing subscription. Unless or until you know you want this, decline.
- Speaking of declining: when installing any of these, always choose custom installation, never the default. The default may include other unrelated software you don't need or want. Consider using Ninite[59] to install the free tools -- all are available there.

---

[50] https://www.malwarebytes.com/mwb-download/
[51] https://go.askleo.com/avg
[52] https://go.askleo.com/avira
[53] Or perhaps not: The Cost of Avast's Free Antivirus: Companies Can Spy on Your Clicks (https://www.pcmag.com/news/the-cost-of-avasts-free-antivirus-companies-can-spy-on-your-clicks, PCMag, January 2020)
[54] https://go.askleo.com/kaspersky
[55] https://go.askleo.com/mcafee
[56] https://www.webroot.com/
[57] https://go.askleo.com/bitdefender
[58] To be clear, I've not run any of the paid versions, and I've not run the "three AVs" in many years. Their mention here is simply based on their reputation over the years.
[59] https://askleo.com/21355

What else besides security software?

A firewall

For home and business use, I recommend the use of any good NAT router as a firewall. You probably already have one.

They don't have to be expensive, and are one of the simplest approaches to keeping your computer safe from network-based threats. If all the computers on the local network side of the router can be trusted, there's no need for an additional software firewall.[60]

When traveling, or if you don't trust the kids' computer connected to the same network as your own, I recommend turning on the built-in Windows Firewall. In recent versions of Windows, it's already on by default. There's no harm in leaving it on, but it can occasionally get in the way of some local machine-to-machine activities, like sharing files and folders.

Back up

I *strongly* recommend you back up regularly.

In fact, I can't stress this enough. Up-to-date backups completely avoid 99% of the disasters I hear about.

Macrium Reflect[61] and EaseUS Todo[62] are the backup tools I currently use and recommend. More on backing up here: How Do I Back Up My Computer?[63]

Stay up to date

Keep your computer -- Windows *and* all the applications you run -- as up to date as possible.

In Windows 10, this happens automatically, as long as you don't take steps to disable it. Needless to say, I strongly recommend you not disable those functions, and let Windows Update keep your system as up to date.

Many of the security issues we hear about are due to individuals (and, sadly, corporations) who have not kept their operating system or applications current with the latest available patches.

And finally, Internet Safety: 7 Steps to Keeping Your Computer Safe on the Internet[64] has even more tips for keeping your computer safe.

[60] https://askleo.com/3484
[61] https://askleo.com/4996
[62] http://todo.askleo.com/
[63] https://askleo.com/6643
[64] https://askleo.com/2374

How Do I Remove Malware from Windows 10 and 11?

One question that shows up almost every day in the Ask Leo! inbox is how to remove malware.

Every day.

The scenarios differ, but the problem is the same: a machine has been infected with spyware, a virus, ransomware, or some other form of malware, and that machine's owner is having a tough time getting rid of it.

Often, anti-malware software is installed that "should" have taken care of it before it got to this stage.

Hopefully, that will never be you.

Let's review the steps I recommend for removing malware *and* reducing the chances it'll happen again.

A word about prevention

If there's one thing I would have you take away from this article, it would be this:

Prevention is less painful than the cure.

As we'll see in a moment, the steps to remove malware can be painful and time consuming. You run the risk of losing data. Knowing how to stay safe on the internet[65] is much, much easier in comparison.

So let's look at what to do when prevention has failed.

Back up

My strong recommendation is to start by taking a complete image backup of your system.

Why would you want to back up a system you know is infected with malware?

A backup taken now is an "it-can't-get-any-worse-than-this" fallback. Some of the techniques we use to remove malware run the risk of breaking things and making the situation worse. With this backup at the ready, you can always restore and start over with nothing lost.

[65] https://askleo.com/2374

Restore a prior backup

If you've been taking regular backups, restoring a prior one is often the most expedient step, and can save a lot of time and energy.

Simply restore your machine completely from the most recent full system backup plus any incremental backups (often handled transparently by your backup software) taken before the infection occurred.

Except for learning from the experience, you're done.

Unfortunately, most people don't have this option available to them. Most people don't begin backing up until after they've experienced data loss or a severe malware infection. One of the lessons they learn is that a recent backup can save them from almost any problem, including malware.

Update the anti-malware database

If you have anti-malware software installed, make sure it's up to date. This includes more than just the software itself; *the database of malware definitions* must also be current.

Almost all anti-malware tools use databases of malware definitions. They change daily, if not more often, and as a result need to be updated regularly.

Many programs will do this automatically, but if for some reason they do not, the program will not "know" about the most recent forms of malware. Make sure the database is up to date so yours does.

Perform a full scan

Anti-malware tools regularly perform a "quick" or fast scan. That's typically sufficient for day-to-day operations.

But not today.

Fire up your anti-malware tools and run a full/advanced/complete scan of your entire system drive. If you have a single tool, that might be one run; if you use multiple tools, such as separate anti-virus and anti-spyware tools, then run a full scan with each. This may take some time, but let the tools do their job.

This also applies if your anti-malware automated scans have stopped working for some reason (that reason often being malware). If this full scan discovers something, it might be worth checking to make sure the security software is properly configured to scan automatically as well.

Try another anti-malware tool

No anti-malware tool catches all malware.

I'll say it again: *there is no single tool that will catch every single piece of malware out there*. None. Some are better than others, some catch more than others, but none of them catch everything.

So using additional reputable tools is a reasonable approach.

I recommend the free[66] version of Malwarebytes' Anti-Malware[67] as the first tool to use. It has a reputation for removing some nasties other tools apparently miss. Once again, run a full scan.

Regardless of which tool you select, *stick with reputable tools.* When a machine is infected, most people tend to panic and download just about anything and everything that claims to be an anti-malware tool. *Don't do that*. There are many less-than-reputable individuals out there ready to take advantage of your panic.

Do some research before downloading anything, or you may just make the problem worse instead of better.

Research specific removal instructions

If your anti-malware software tells you the *name* of the specific malware you're dealing with, that's good information—even if it can't remove it.

Search for that malware, and you're likely to find specific removal instructions at one or more of the major anti-malware vendor sites. These instructions can be somewhat technical and intimidating, so take your time to follow them precisely, or get a techie friend to help.

Those instructions often come with offers to remove the malware—for a price. As long as it's an *option* (in other words, the manual removal instructions are also provided), then it may be a viable alternative if the company is one you trust. On the other hand, if all you're presented with is a promise and a price, move on.

Some sites offer free tools you can download to remove specific malware. Once again, *use caution*. When the tools are from reputable sources, they're a quick way to avoid some hassle. When the tools are really just more malware in disguise, they'll make your problems worse.

If you download anything to help address the problem, make sure that wherever it comes from, it's an organization you know and trust.

Surrender

This is the only sure-fire way to remove any virus. 100%. Guaranteed.

---

[66] Yes, there is a truly free version. See the Malwarebytes article for details.
[67] https://askleo.com/5765

In fact, it's the only way to know that you've removed a virus. Once infected, none of the steps above are guaranteed to remove malware, even if they report that things are clean. Once infected, all bets are off. An infection can fool anti-malware software into thinking that everything is fine even when it's not.

There's just no way to know.

The only way to be absolutely positive that you've removed any and all viruses is:

- **Back up**. If you haven't already, back up the entire system. You'll use this to restore your data after we're done.
- **Reformat**. Reformatting erases the entire hard disk of everything: the operating system, your programs, your data, and most important of all, all malware. This may be part of the next step, as most Windows set-up programs offer to reformat the hard drive before installing Windows.
- **Reinstall**. Yes, reinstall everything from scratch. Reinstall the operating system from your original installation media or download. Reinstall applications from their original media or downloads saved elsewhere.
- **Update**. Update everything, in particular making sure to bring Windows as completely up to date as possible for the most current protections against all known and patched vulnerabilities. Applications, particularly your anti-malware tools, should be updated as well.
- **Restore**. Restore your data by carefully copying it from the backups you created when we started. By "carefully," I mean take care to only copy the data you need, so as not to copy back the malware—don't copy potential sources of infection. It's true there is no guarantee you won't copy the malware back, so copy only what's absolutely needed, and make sure your anti-malware tools are running and up to date.
- **Learn**. Take stock of how this happened, what you might have done to get infected in the first place, and what might have helped you recover more efficiently. Consider instituting a frequent system backup.

It's not your fault, but it is your responsibility

By now, I hope you can see why prevention is so *much* less painful than the cure.

Taking a few extra steps to keep things up to date, avoiding those cute virus-laden downloads and attachments, and learning how to stay safe [68]is *much* easier than the recovery process I've just outlined.

[68] https://askleo.com/2374

And having backups[69] can make the recovery process as close to painless as possible if you do get infected.

Yes, it's not your fault. But *it is your responsibility* to learn the basics about staying safe when you use your computer.

In an ideal world, we'd never have to worry about malware, or the "bad guys" trying to fool us into doing things we really shouldn't. But you already know this isn't an ideal world; software isn't perfect and never will be. There will always be someone out to scam the vulnerable.

Even though it's not your fault, you still need to be the one to get educated and take the steps needed to stay safe.

Right or wrong, it's just a practical reality.

[69] https://askleo.com/6643

How Do I Remove PUPs and Other Unexpected Things From My Computer

Ending up with random software on your machine that you never wanted in the first place is annoying as all heck.

So-called PUPs (for Potentially Unwanted Programs, although there's rarely any "potentially" about it) are tools, settings, utilities, browser toolbars, extensions, and more software installed on your computer as a result of installing something else. PUPs are rarely even related to what you're installing.

I'll talk a little about prevention, but first, let's walk through the steps I recommend when you suddenly realize you've been saddled with software you didn't know you'd agreed to and certainly never wanted.

Start with a backup

The steps we are about to take have a small chance of causing problems.

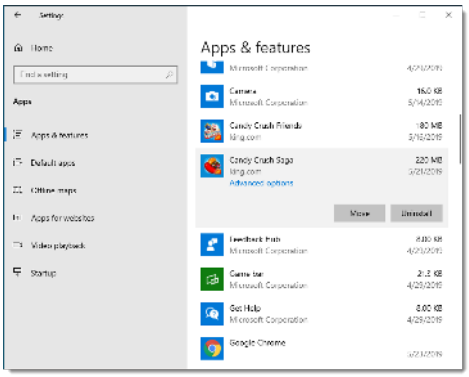
Whenever that's the case, I strongly recommend you take a full image backup of your machine before you do anything else. That way, you'll have that backup to restore should anything below go wrong.

Uninstall the somewhat well-behaved PUPs

A number of unexpected toolbars and other applications that show up on your machine are "relatively" well behaved; by that I mean they are somewhat easy to uninstall using official mechanisms.

Start in the Windows Settings app, and click on **Apps**.

Look for the item by name. Sometimes that can be tricky, as applications are intentionally named obscurely to make them more difficult to remove, but the well-behaved items we're looking for here should be relatively clear. Look for names that include the word "toolbar", in particular, as those are some of the browser-behavior-altering pests that often put us in this scenario.



Right-click the item you want to uninstall, and click Uninstall.

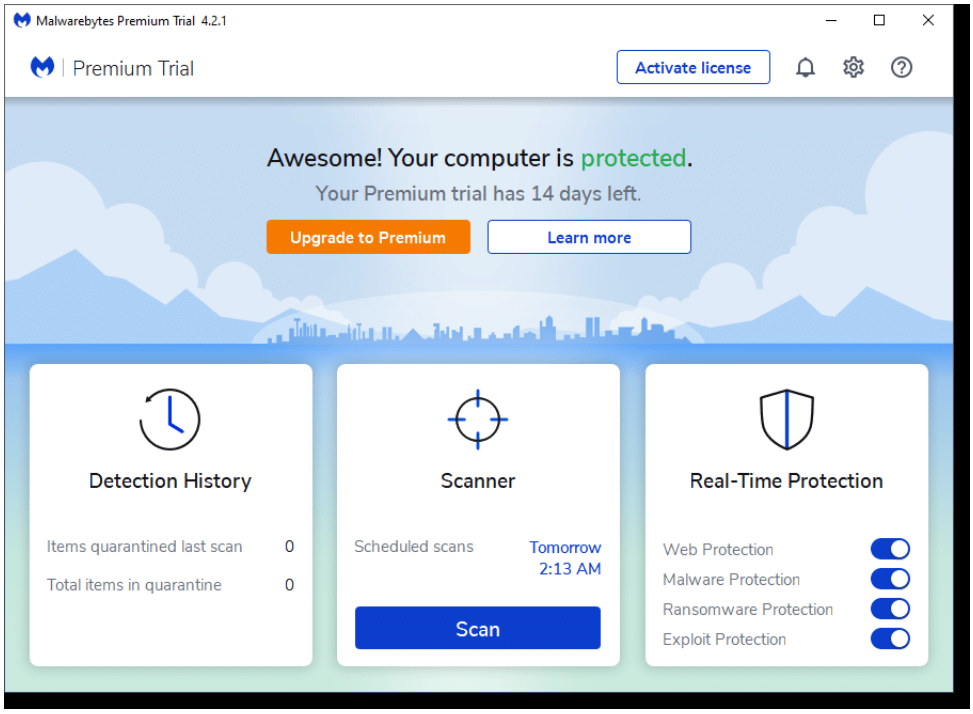
We'll do the next steps even if it appeared to work, because in many cases there will be traces left over, and sometimes those traces can reinstall the PUP.

Run Malwarebytes

If you don't have it already, download and install the *free* version of Malwarebytes Anti-Malware.[70]

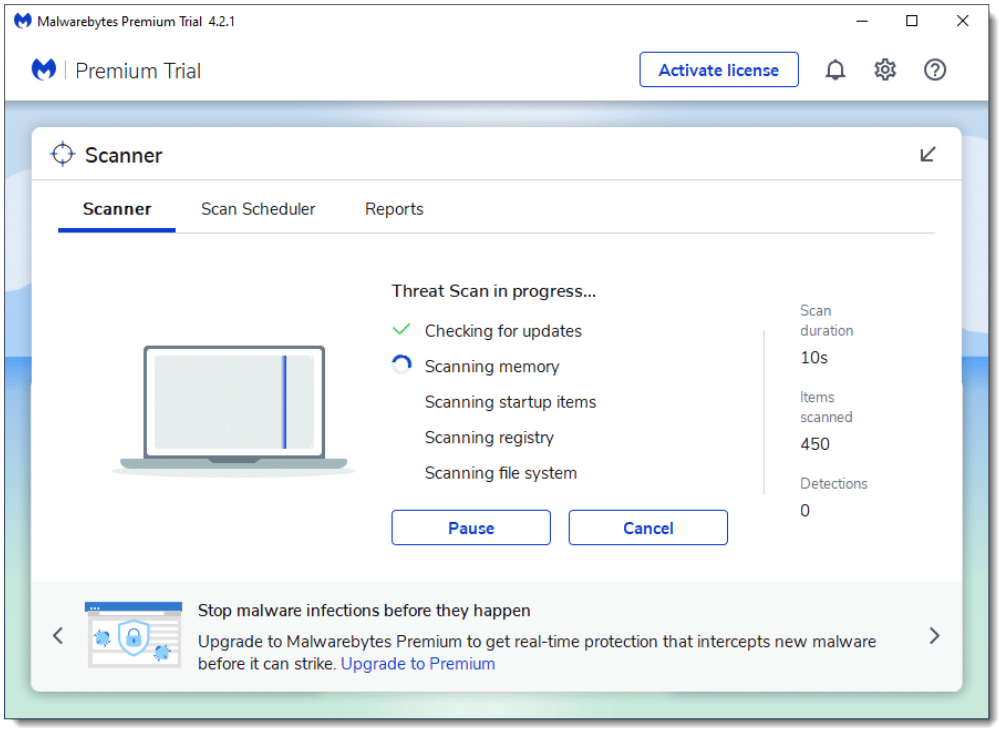
Important: The free version is, at first, a free trial of their paid version. It will nag you to register/upgrade/license the product. *You do not need to do so.* Simply use the product as described here. After a period of time (two weeks, at this writing) the trial will revert to the purely free version. It may continue to nag you, but it will keep working.

Run the program, if it hasn't started automatically, and click Scan to perform a scan.



The Malwarebytes scan may take a while.

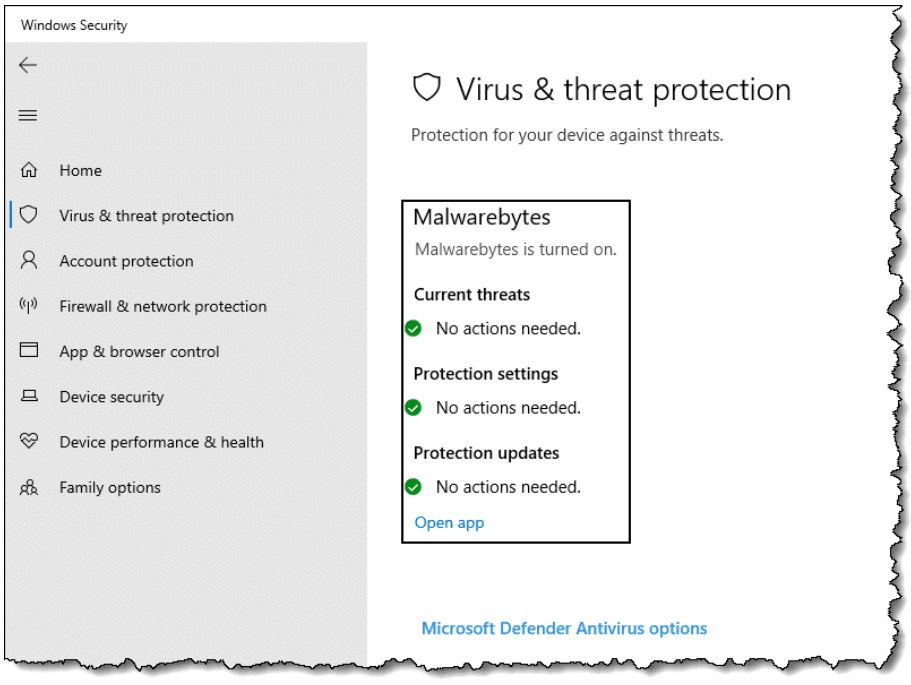
[70] http://www.malwarebytes.org/free/



When it's complete, you'll get a notification if you have malware or PUPs.

Even if no actual malware is detected, potentially unwanted programs—PUPs—may still be found. Malwarebytes will show you the entire list. You can review the list if you like, but in general, the correct next step is to simply quarantine everything. You will likely need to reboot.

A clean scan is your goal.



Note that you may want to uninstall Malwarebytes, as its trial version will have disabled Windows Defender in Windows Security. This isn't really a problem; you shouldn't have two real-time security solutions running at the same time, and Windows Security knows to step aside when Malwarebytes is installed. That being said, if you don't plan on keeping Malwarebytes, you'll probably want to remember to uninstall it when all is said and done. If you don't, after the trial period it will step aside; Windows Security will resume full real-time protection, and Malwarebytes will remain available for on-demand scans.

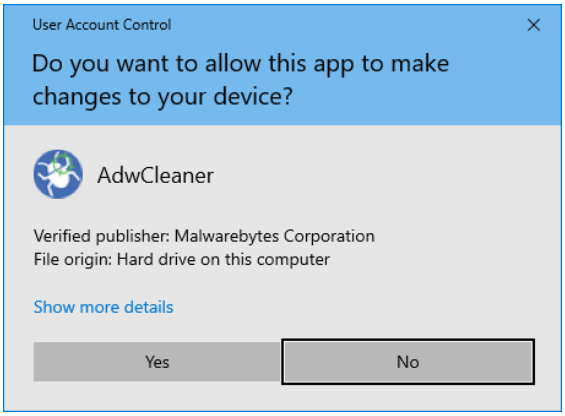
It's possible that Malwarebytes is unable to remove some PUPs. If that's the case (or even if it's not), I still want you to take one more step.

Run AdwCleaner

AdwCleaner is perhaps best downloaded from our friends over at BleepingComputer.com.[71] (AdwCleaner was purchased by Malwarebytes in 2016, but remains a separate tool.)

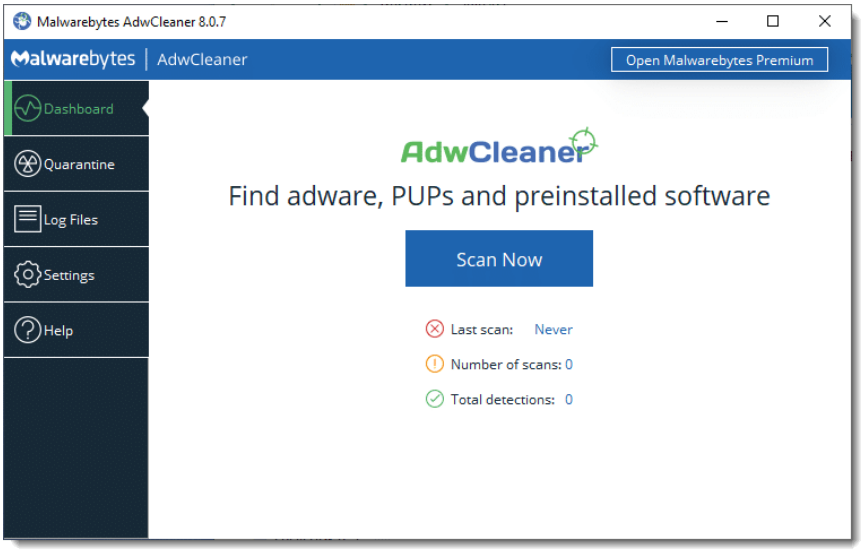
Speaking of being careful, remember to avoid advertisements that say "Download" or "Free Download." Those are *not* the programs you want. The button that I used simply read, "Download Now @BleepingComputer."

AdwCleaner has no install. Once downloaded, simply run it, and answer Yes to any UAC prompt.



Also click **I agree** to any licensing terms agreement. Click **Scan Now**.

[71] https://go.askleo.com/adwcleaner



Once the scan is complete, AdwCleaner will present its scan results.

If you're not certain about what AdwCleaner finds, go ahead and let it clean up anything you don't recognize by clicking **Clean & Repair**. (It first warns you that all programs should be closed.)

The ultimate removal

Even with the tools I've outlined, and other tools that may also be used or may come along later, there's a real possibility that the unwanted software will *still* not be completely or successfully removed. This often happens when the PUP is new and the security-software makers are still catching up to the latest tricks it might be playing.

It's worthwhile to consider restoring to a recent backup image.[72] Restoring will make these things go away *every single time*.

If you have a back-up image of the machine as it was prior to these pests having been installed, you can simply restore your machine to that image, and they're gone. No fancy tools are needed, and you needn't just hope that it works. Restoring to a prior backup works *every time*.

Presuming, of course, you have one.

Prevention

PUPs and related pests arrive in several different ways, but most commonly, they are "offered" to you when you install[73] or even update[74] something else. Often, the offer is hidden and defaulted to Yes. The technical loophole is that by choosing this default (or not unchecking the appropriate box) when you install some program you've downloaded, you're actually *asking* for this other software, these PUPs, to be installed.

[72] https://askleo.com/6643
[73] https://askleo.com/4906
[74] https://askleo.com/24027

Don't do that.

Whenever you install any software—*even software you've purchased*—always choose the "Custom" or "Detailed" option. Choose whatever option is *not* the default option.

Then pay very close attention to every option you're presented. If it offers you something that is not clearly related to the software you want, *uncheck it*. If it offers to change your search page, *uncheck it*. If it offers to install some toolbar, *uncheck it*.

You get the idea.

The bottom line is, if you're not careful when you install software—even software from reputable vendors—you may end up with things you never expected or wanted.

There's nothing "potentially" unwanted about it.

Will Using an On-Screen Keyboard Stop Keyloggers?

> *"Will using the on-screen keyboard in Windows stop keyloggers?*

The short answer is very simple: *no*.

I get a surprising amount of push-back on this, but the simple truth remains: while it might stop some, it's nothing you can count on to be 100% effective.

Keyloggers are a form of malware that record your keystrokes to capture things like your login usernames and passwords so hackers can get into your accounts. Let's look at the path of keystrokes from your finger to your computer to see the various ways your keystrokes can be intercepted and logged.

The keyboard connection

Typically, when you type a key on your keyboard, a microprocessor within it sends signals via the cable connecting it to your computer.

Here we encounter the first point of vulnerability. No, not the microprocessor in the keyboard (technically possible, but exceptionally unlikely)—but the cable, or rather, what the cable plugs into.

Particularly lucrative targets are public computers, where someone comes along and installs a *physical device* between the computer and keyboard, a device that intercepts and logs every keystroke entered. Sometime later they come back, remove the device, and take with it all the information users of that computer entered.

As it turns out, wireless keyboards can be worse. Wireless keyboards *broadcast* the keystrokes you're typing. Any receiver within range can "listen in". Wireless keyboards do encrypt their data, so in theory, the information should be safe, but the quality of the encryption can vary based on the age of the keyboard and the vendor. In addition, the concept of “in range" turns out to be much further than most people think, particularly for a thief with equipment dedicated and tuned to this purpose.

The good news is that your on-screen keyboard protects you against these two specific types of keyboard-related threats. By using the on-screen keyboard, you bypass those components of the keyboard hardware that could be compromised.

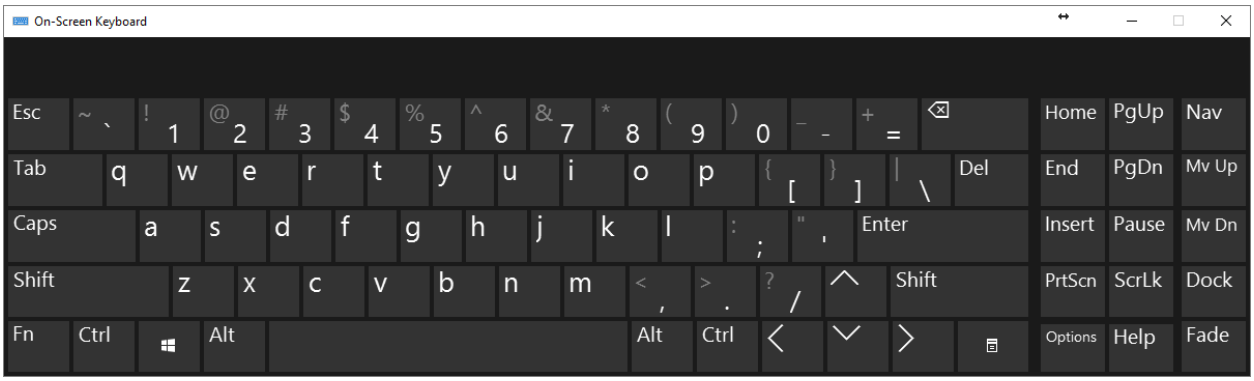
The bad news is that hardware-based keyloggers are rare. Much more common are software-based threats.

The keyboard software

Once your keystrokes arrive at the computer from the keyboard, they are processed by a keyboard device driver which (to oversimplify) handles the translation of the keyboard "scan codes", as they're called, to the letters, numbers, and symbols Windows applications expect.

Keyloggers typically insert themselves into the receiving end of this process: they get the keystrokes from the keyboard as they are passed on to Windows.

This is where the on-screen keyboard scenario gets interesting.



The on-screen keyboard application is a "virtual" keyboard. It has its own device driver, which, to Windows, "looks like" a real keyboard.

As a result, the keystrokes it sends to Windows can easily be captured by the same key-logging software capturing keystrokes from the real keyboard, if that keylogger has installed itself in the proper place.

A keylogger is just malware

Perhaps the most important concept to remember here is that keyloggers are just another form of malware.

And malware can do *anything.* Keyloggers can capture much more than just keystrokes.

You use the virtual keyboard by using your mouse to point and carefully click at the image of a key on the keyboard. A keylogger could, then, for every mouse click:

- Capture the location of the mouse on the screen.
- Capture a screenshot image of the screen, or just the area "around" the mouse pointer.

The keylogger has captured a series of images showing exactly where you clicked and in what order. In other words, it's captured your virtual keystrokes.

Note that this approach to keylogging also bypasses one of the more common so-called security techniques of randomizing the keyboard layout on the screen. You still have to be able to see where to click, and the logger simply logs what you see and where you click, regardless of how the keyboard is laid out.

Keyloggers as threats

How big a threat is all this?

It depends who you ask. In my opinion, "normal" keyloggers—those that record only keystrokes—are a fairly common threat, and are one reason why anti-malware protection, general internet safety, and the use of common sense in general is so important. So yes, they're out there.

The real question is, how pervasive are the more sophisticated keyloggers, which do more than capture keyboard keystrokes, but use other techniques to effectively achieve the same result?

It's hard to say, but I have to say it again: keyloggers are "just" malware. If they're on your machine at all, you have a problem, and that problem may not be limited to logging what you type.

Like any malware, you might not even realize they're there until it's too late. As a result, focusing on solutions targeted only at thwarting keyloggers is not only fundamentally misguided, but it also diverts your attention from a much bigger problem: if you have a keylogger, *you have malware*.

Focus on avoiding or removing malware of all sorts, and you'll be avoiding or removing keyloggers as a side effect.

Do not rely on a virtual keyboard of any sort as a security measure.

Protecting with Updates

How Do I Make Sure Windows is Up to Date?

> *"How do I make sure Windows is up to date? And... should I?*

The last question is easy to answer: yes. Yes, you absolutely should keep Windows as up to date as possible.

I know there are those who disagree. Some go so far as to seek out ways to prevent Windows from updating itself.

Let's look at why they feel that way, and what I believe you should do. This article focuses on Windows 10 and 11.

Vulnerabilities and updates

The issue is common to all software: no one is perfect. All software has bugs, period, no exceptions.[75]

While many bugs are inconsequential, some make the software vulnerable to exploitation by people trying to do something bad, like hack into your system, steal your data, use your computer to send spam, or worse. These bugs are often referred to as *vulnerabilities*, and the software taking advantage of them is termed *malicious software*, or *malware* for short.

When vulnerabilities are found, manufacturers release updates to their software that fix (or *patch*) the bug.

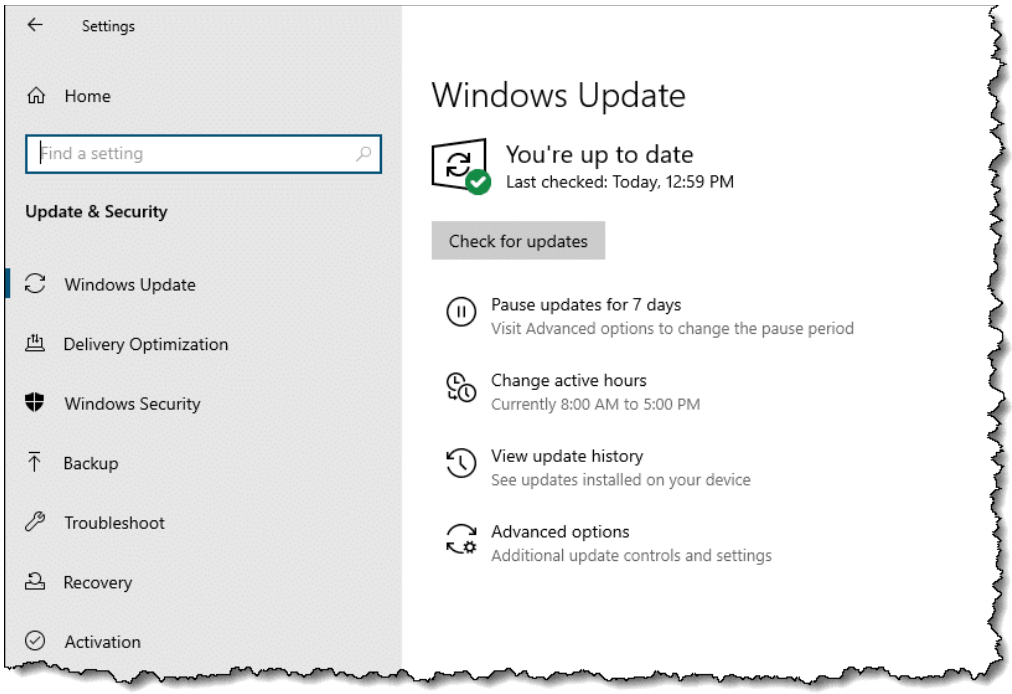
It's important that users of affected software install those updates when they're made available.

Unfortunately, some individuals do not install updates for a variety of reasons. This leaves their computers vulnerable to more and more malware, even though the associated bugs the malware can exploit have been fixed.

Automating updates

Windows Update is Microsoft's solution to update distribution and installation.

[75] If someone claims that a particular bit of software has no bugs, then either they simply haven't yet found the bugs that are there anyway, or they've dismissed some erroneous or unexpected behavior (aka a bug) as not rising to the level of being called a bug. It's still a bug.



It runs in the background, periodically checking for updates to Windows[76] that apply to your machine's particular configuration. When available updates are found, Windows Update downloads and installs them automatically.

It's not uncommon for updates to require your machine to be rebooted. Software cannot be updated if it's in use. That means in order to update core components of Windows itself, Windows needs to shut down briefly. That's a reboot.

Updates and failures

I said earlier that all software has bugs.

Updates are no exception. They are software, so they could have bugs. The update process itself could have bugs.

The net result is from time to time, or perhaps from person to person, Windows Updates are sometimes considered risky. There's a perception that with any update, there's a risk your machine could become less stable. In the worst cases, Windows updates have completely crashed the machine on which they've been installed.

That bad reputation — warranted or not — has had serious long-term consequences.

[76] And, optionally, other Microsoft software.

Perception and reality

Windows 10 is installed on close to, if not over, a billion machines world-wide. That means when there's even a hint of a problem, it makes headlines everywhere. The size or scope of the problem is immaterial to the headline writers; every failure is treated as a big deal, if not a disaster.

To be fair, even if one tenth of one percent of all Windows 10 machines suffered a failure due to Windows Update, that's still a million machines. That's a lot.

And yet, everything else being equal,[77] you run only a 1 in 1,000 chance of having a problem.

Still, because of headlines and reputation, some users delay updates to what they consider a safer time — a few days or weeks later. In some cases, they try not to take updates at all.

Malware authors approve. To them, delaying or skipping updates means once a vulnerability is discovered, they can continue to write and circulate malware to exploit it, because they know not everyone will take the update to fix it. If you pay attention to notifications of large data breaches in the news and dig deep enough, you'll often find that hackers gained access via a vulnerability for which a patch had been made available but had not yet been applied.

Applying updates regularly remains the best approach to keeping your system secure and up to date. I continue to recommend you let Windows update itself automatically, so you don't have to take any action at all.

Forced automated updates and your options

Windows 10 originally had no option to delay updates in its consumer ("Home") editions. Updates were downloaded and installed automatically.

In a perfect world, this would be a perfect solution. Unfortunately, we do not live in a perfect world.

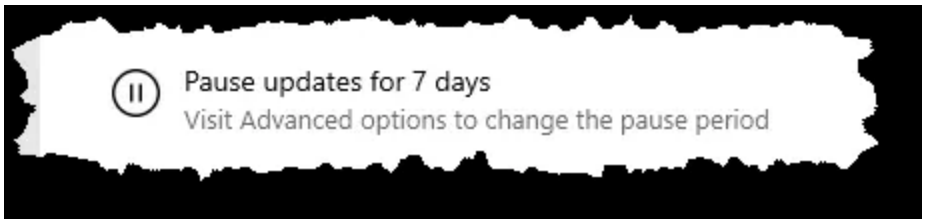
There have been two major issues:

- While the stability of Windows updates have improved over time — fewer and fewer updates cause significant problems — some Windows updates, at least initially, seemed a step backwards. Reports of people having problems after an update seemed to increase.
- Updates requiring a reboot would indeed reboot, often at an inconvenient time.

The stability of updates appears to be improving once again, and Microsoft has made additional options available.

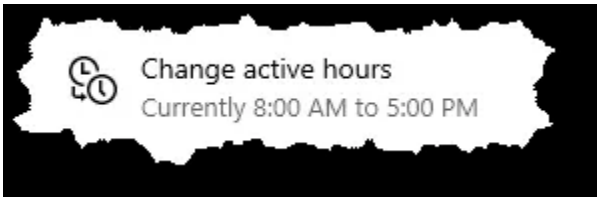
In Settings, Windows Update, you'll find an option to "Pause updates for 7 days."

[77] With no specific characteristics to refine the number, it's 1 in 1,000. However, it often becomes quickly apparent that a failure applies to certain machines, or certain characteristics of machines, meaning you can much more accurately judge the risk you face. Typically, you have even less risk than 1 in 1,000.



This is particularly useful if your computer usage is about to be particularly sensitive or important; you know you won't be impacted by an update.

Similarly, Microsoft added the concept of active hours.



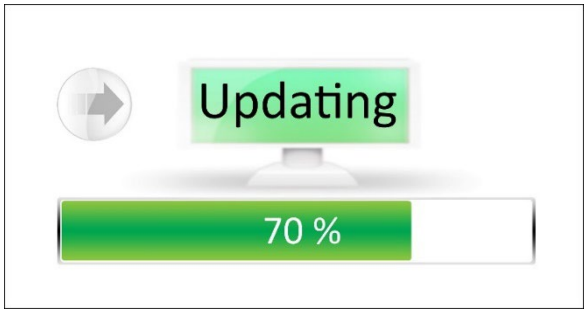
This allows you to tell Windows Update when you normally use your computer. It will not reboot the computer during this time.

In **Advanced Options**, you'll find the following options.

- "Show a notification when your PC requires a restart to finish updating." This allows you to control when your machine will reboot, allowing you to save your work and make sure nothing will be negatively impacted by the reboot.
- An option to pause updates. This is the same as the setting above, but allows you to pause updates for up to 35 days if need be.

The bottom line is that Microsoft really, really, REALLY wants you to keep your machine as up to date as possible. And I agree.

Recommendation: managing risk



It's all about risk management: trading off the risk of a misbehaving update to the risk of having an unpatched vulnerability exploited by malware.

The good news is, we know how to manage risk.

For all versions of Windows, my recommendation remains:

1. Back up[78] regularly. Ideally, perform system image backups[79] as I've outlined in several articles. Then, no matter what, you're protected from any kind of failure, be it hardware failure, a crashed disk, malware, or even a troublesome Windows update.

[78] https://askleo.com/6643
[79] https://askleo.com/4473

2. Configure Windows to notify you when a restart is required, and restart as soon as is practical. This places the restart and its impact completely under your control.
3. Don't delay updates if you don't have to, and if you do, choose the smallest length of time you can. This minimizes the length of time you leave your machine exposed to known vulnerabilities.
4. Don't try to disable Windows Update. It's critical to your safety.

In my opinion, this is the safest approach to managing a wide variety of risks related to using your computer—not just the risks of a failed update.

Part 4: Protect Your Laptop

How Do I Use an Open Wi-Fi Hotspot Safely?

> *"I've returned to the same coffee shop where I was a few months ago when I noticed that my email had been hijacked/hacked. This time, I'm using my phone, but the last time, when I noticed the hack, I was using my computer and doing email over an open-internet, free Wi-Fi network.*
>
> *Do you think that could be the source of the problem or just a coincidence? I'm still afraid to do email from here.*

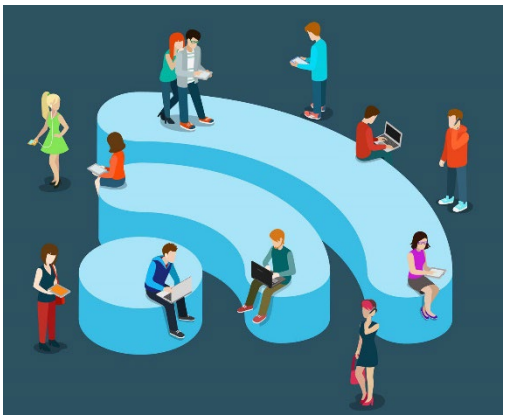
It definitely could have been.

Unfortunately, it's hard to say for sure, and it could have been something else.

As we can't really diagnose the past, let's look ahead instead.

It can be absolutely safe to send and receive email, or even other tasks, from a coffee shop or other location that provides unsecured or "open" Wi-Fi. In fact, I do it all the time.

But you do have to follow some *very* important practices to ensure your safety.



The open Wi-Fi problem

The problem with open Wi-Fi hotspots is that the wireless radio connection between your computer and the wireless access point nearby is not encrypted. That means any data you don't actively encrypt some other way is transmitted in the clear, and *anyone within range can eavesdrop* and see it. Encryption prevents that.

Important: know if it is encrypted or not. If you connect to a hotspot and the operating system on your machine requires a password for it to work — say with a password provided by the barista or hotel clerk — that's not an "open" Wi-Fi hotspot, and you may be OK. When you're required to provide a password before you can connect, the Wi-Fi access point is using some form of encrypted connection.

On the other hand, if you can connect without a password, and your browser immediately takes you to a webpage that says "Enter a password" (as in a hotel) or "Check to accept our terms" (as in many other open hotspots) *it is not encrypted and it is not secure*. It is an open Wi-Fi hotspot.

Turn on the firewall

Fortunately, firewalls are "on" by default in most operating systems.

However, when you're at home, you may use your router as your firewall, and keep any software firewall on your machine disabled. That works well, as the router stops network-based attacks before they ever reach your computer… while you're at home.

But when you're on an open Wi-Fi hotspot or connected directly to the internet via other means, that software firewall is *critical*.

Make *sure* your firewall is enabled before connecting to an open Wi-Fi hotspot.[80] Various network-based threats could be present on an untrusted connection, and it's the firewall's job to protect you from that.

Secure your desktop email program

If you use a desktop email program, such as Outlook, Windows Live Mail, Thunderbird, or others, you *must* make certain it is configured to use SSL/secure connections for sending and downloading email.

Typically, that means that when you configure each email account in your email program, you need to:

- Configure your POP3 or IMAP server for accessing your email using the SSL, TLS, or SSL/TLS security options, and usually a different port number.
- Configure your SMTP server for sending email using SSL, TLS, or SSL/TLS security options, and usually a different port number.

How you configure these settings depends on the email program you use. The specific settings depend on the email service.

Once configured with the proper settings, you can feel secure downloading and sending mail using an open Wi-Fi hotspot.

Secure your web-based email

If you use a web-based email service like Gmail, Outlook.com, Yahoo, or others via your browser, you *must* make sure it uses an httpS connection. Fortunately, most all major email services now rely on https.

In years past, accessing email using a plain http connection might well have been the source of many open Wi-Fi-related hacks: usernames and passwords are visible to any hackers in range who cared to look. Https prevents that.

Secure all your other online accounts

Any and all web-based (aka "cloud") services that require you to log in with a username and password should either be used only with https from start to finish or be avoided completely while you're using an open Wi-Fi hotspot.

[80] https://askleo.com/2689

With more and more services provided online, this is getting to be a larger problem. Fortunately, most are aware of the issue and are using https properly.

Using the cloud is a great way to manage your digital life from wherever you may be, but security remains key. Using https is critical when you're out and about.

Use a VPN

This one's for the road warriors. You know them: the folks who are always traveling and online the entire time, often hopping from coffee shop to coffee shop in search of an internet connection as they go.

A VPN, or Virtual Private Network, is a service that sets up a securely encrypted 'tunnel' to the internet and routes *all* of your internet traffic through it. Https or not, SSL/secure email configuration or not, all of your traffic is securely tunneled, and no one sharing that open Wi-Fi hotspot can see a thing.

This service typically involves a recurring fee.[81] As I said, they're great for road warriors, but probably overkill for the rest of us, as long as we follow the other security steps described above.

A VPN also has the side effect of protecting you not only from the hacker in the corner but from the coffee shop IT guy or whoever is providing the internet connection.[82]

Use different passwords

Finally, it's important to keep your account passwords different from each other[83] and, of course, secure.[84]

That way, should one account be compromised by some stroke of misfortune, the hackers won't automatically gain access to your other accounts.

Remember, even when you use an open Wi-Fi hotspot properly, a hacker can still see the sites you're visiting, even though they cannot see what you are sending to and from that site. That means they'll know exactly what sites to target next.

Consider not using free Wi-Fi at all

As I said, it can be safe to use open Wi-Fi, but it's also very easy for it to be unsafe.

One very common and solid one solution is to use your phone instead.

---

[81] In fact, I'd avoid free VPNs, as they run a higher risk of tracking or exposing your information in other ways.
[82] https://askleo.com/3004
[83] https://askleo.com/11788
[84] https://askleo.com/4844

While it is technically possible, a mobile/cellular network connection is *significantly* less likely to be hacked. In fact, I use this solution heavily when I travel.

Most mobile carriers offer one or more of the following options.

- **Use your mobile device**. Many phones or other mobile devices, such as iPhones, iPads, Android-based phones, and others, are quite capable email and web-surfing devices, and typically do so via the mobile network. (Some also use Wi-Fi, so be certain you're using the mobile broadband connection to avoid the very security issues we're discussing.)
- **Tether your phone**. Tethering means you connect your phone to your computer—usually by a USB cable, but in some cases, via a Bluetooth connection—and the phone acts as a modem, providing a mobile broadband internet connection.
- **Use a dedicated mobile modem**. These are USB devices that attach to your computer and act as a modem to provide a mobile broadband internet connection, much like tethering your phone.
- **Use a mobile hotspot**. In lieu of tethering, many phones now have the ability to act as a Wi-Fi hotspot themselves. There are also dedicated devices, such as the MiFi, that are simple dedicated hotspots. Either way, the device connects to the mobile broadband network and provides a Wi-Fi hotspot accessible to one or more devices within range. When used in this manner, these devices are acting as routers and must be configured securely,[85] including a WPA2 password, so as not to be another *open* Wi-Fi hotspot susceptible to hacking.

I travel with a MiFi and have a phone capable of acting as a hotspot as a backup. I find this to be the most flexible option for the way I travel and use my computer.

Don't forget physical security

Laptops are convenient because they're portable. And because they're portable, they're also easily stolen.

Unfortunately, it only takes a few seconds for an unattended laptop to disappear. I never leave mine alone: even if I need to make a quick trip to the restroom, the laptop comes with me. There's just no way of knowing that absolutely everyone around me is trustworthy.

In that same vein, I also prepare in case my laptop does get swiped. Specifically, that means:

- My hard drive is encrypted.
- My sensitive data is stored in folders that are encrypted using BoxCryptor. Those folders are not mounted unless I need something.
- 1Password, my password management software, is set to require a password re-prompt after a certain amount of inactivity.
- I have two-factor authentication enabled on as many accounts as support it, including 1Password.
- I have tracking/remote wiping software installed.

[85] https://askleo.com/11107

Computer theft and recovery is a larger topic that's only tangential to using open Wi-Fi hotspots. Clearly, though, if you are a frequent user of assorted open hotspots in your community or when you travel, a little attention to theft prevention and recovery is worthwhile.

Security and convenience are always at odds

As you can see, it's easy to get this stuff wrong, since doing it securely takes a little planning and forethought.

But it's important. If you're not doing things securely, that guy in the corner with his laptop open could be watching all your internet traffic on the Wi-Fi connection, *including your account username and password* as they fly by.

And when that happens, you can get hacked.

Fortunately, with a little knowledge and preparation, it's relatively easy to be safe.

How to Protect Data on a Laptop

> *"How can you set a strong password in a laptop so that data can't be stolen?*

Protecting the data on your laptop takes much more than a strong password. In fact, it takes at least a couple passwords, plus some settings, plus some encryption on top of it all.

Given that laptops are so easily lost and/or stolen, let's walk through the four steps I recommend to protect the valuable data you have stored on it.

1. Lock your UEFI[86]

If your computer's UEFI[87] supports it, configure it to require a password to be able to boot. This prevents strangers from even starting your machine, much less accessing what's on it directly.

Exactly how you do it will vary depending on the make and model of your computer. Not all UEFI interfaces are the same, and not all support the same set of features. Check with your computer's manufacturer for specifics. If you're able to set one, *do not* forget the password.[88]

This will not only prevent someone from accessing what's on the machine but will also prevent them from making changes to the machine. For example, with a BIOS password set, they should not be able to change the boot order and boot from anything other than the settings you've chosen.

While you're at it, turn on Secure Boot,[89] if it's not already on. This restricts the computer from booting into untrusted operating systems or installing unauthorized UEFI replacements. Caution: turning Secure Boot on or off may change how your system boots and render the operating system inaccessible. If this happens, simply revert the change and the machine should return to normal. Consider setting Secure Boot prior to your next operating system installation if this happens.

2. Lock your hard disk

This is the single most important step on this list. By "lock your hard disk", I mean use whole-disk encryption. This can take any of several forms:

- Windows BitLocker,[90] if your edition of Windows supports it.[91] Make absolutely certain to back up the encryption key when offered.
- VeraCrypt whole-disk encryption.[92] As it is passphrase-based, do not lose or forget the passphrase.

[86] I'll use UEFI to refer to both UEFI and BIOS.
[87] https://askleo.com/glossary/uefi/
[88] https://askleo.com/4777
[89] https://go.askleo.com/secureboot
[90] https://askleo.com/17437
[91] BitLocker is not available in Home editions.
[92] https://askleo.com/27408

- A hard disk encrypted at the hardware level. This manifests much like a UEFI password: you must specify a passphrase prior to being able to boot from the drive. Once again, do not lose the passphrase.

Encryption is the ultimate protection for your data. Even when all else fails and a hacker or thief makes off with the hard drive from your machine, they still won't be able to access the data on it without knowing the passphrase or encryption key.

Neither will you, should you ever lose the key or forget the passphrase… so don't.

3. Lock your login

You should have a strong password for your computer's login, particularly if you use a Microsoft account. Unlike a local machine account, your Microsoft account is also accessible — and therefore vulnerable — online.

Using additional login methods — like a PIN or facial recognition — is something I discourage for mobile computers with sensitive data. They represent additional places hackers can poke and prod. Guessing your strong password is unlikely, but a short PIN can easily be exposed in other ways. It concerns me that a good photo might squeak by facial recognition tools, so I'd avoid it as well.

Long, strong passwords remain the best protection.

While you're at it, make sure there are no additional login accounts enabled on your machine. If the normally hidden account called "administrator" is enabled, disable it (assuming your normal login account is administrator capable).[93]

4. Lock your machine

When traveling, a friend of mine never leaves his laptop alone without physically locking it to something else in the room, like a table.

Most laptops have a slot for what's called a Kensington lock.[94] It's a standard design to securely tether mobile devices in place.

Even with all the precautions already taken — UEFI passwords, encrypted disks, and secured accounts — it's still important to make sure the laptop itself can't be stolen.

As I've said many times, if it's not physically secure, it's not secure.

[93] https://askleo.com/4757
[94] https://go.askleo.com/kensington

A story from the trenches

Much of the above came to mind when a friend handed me a laptop and asked me to see if I could make it usable again. It had been part of a corporate network that they no longer had access to, so they could not sign in. They just wanted to be able to use the machine for themselves, and didn't really care about what was on it; any photos could be restored from copies on their mobile phone.

I discovered the machine's hard disk had been encrypted using BitLocker, and of course we did not have access to the corporate encryption key. The result? The data on the machine was completely inaccessible. I was able to back up the hard disk, but the encryption remains in place. I'm not sure the backup will ever be useful, other than to restore the machine to the state it was in when I got it.

On the other hand, without needing a UEFI password, I was easily able to change the boot order and boot from a Windows 10 setup drive. This allowed me to install Windows 10 from scratch and erase everything on the drive, encrypted or not.

I hate to harp on it, but…

Much of what I've described above relies on an encryption key, passphrase, or strong password.

Do not lose them. If you do, you will be the one locked out, and everything on your machine may be rendered inaccessible. That's the whole point of this type of security.

There are no back doors.

I mention this — again — because of the fairly constant stream of questions from folks wanting to get into accounts or devices for which they've lost their passwords, passphrases, or encryption keys.

Part 5: Protect Your Online World

Please Set Up and Maintain Account Recovery Information

It might be as important as backing up.[95] It's certainly close.

The number of people I hear from desperately trying to regain access to their accounts would surprise you.

The number of people who will never regain access[96] would surprise you more. I see it at least daily.

It doesn't have to be that way!

Recovery information has one purpose

You know you are who you say you are.

If you lose your password, all indications are that you are not who you say you are. If you were the rightful account holder, after all, you would know the password.

I know, I know! That's not the case if someone has hacked you or you lost that little green notebook with all your passwords scrawled in it. But the service has no way of knowing that. Your username/password combo[97] is how you prove to them you are who you are.

What most services do realize, though, is that people are people. Sometimes we forget our password. Sometimes our accounts are hacked.

Recovery information is an alternate means for you to prove you are who you say you are and should be given access to the account.

You must set up recovery information before you need it

The reason recovery information works is because you set it up *while you have access to your account*. It's information you add to the account in case of future problems.

Hopefully, you'll never need to use it. But you must set it up just in case.

If you never set it up, then should your password ever stop working, *you'll have no way to prove you are authorized to access the account.*

You must keep recovery information up to date

Honestly, most people facing account loss due to failed recovery attempts did set up recovery information when they set up their accounts. That's good, but it's not enough.

---

[95] https://askleo.com/30103
[96] https://askleo.com/15584
[97] Plus your second factor, if you have that configured.

Many of these accounts are years old (and that's one reason you care so much about it). The recovery information you might have configured back then falls out of date. Maybe your recovery phone number is no longer in use, or your recovery email address has long since disappeared, for example.

Out-of-date recovery information is just as bad as not having it at all. It might even be worse if it gives you a false sense of security.

You must keep it up to date. Check it periodically (some services now occasionally prompt you to do this), and/or proactively update it when something changes.

Type of recovery information

Here are the kinds of things we're talking about here.

Alternate email addresses. Make sure you still have access to the email account to which the recovery code will be sent. If you do not, recover *that* account or configure a different one.

Mobile phone number. Contrary to conspiracy-minded folks, this is not used to gather more tracking data on you. (The mobile services already have plenty.) Make sure that any mobile number configured in your account is a number at which you can currently receive a text message. If you change numbers, make sure to change your recovery information. If you lose your mobile, replace it quickly and have your phone number ported to the new device; text messages are tied to your mobile number, not a specific device.

Landline phone number. This is less common, but some services allow you to use a landline and call you with a recorded confirmation code in case of recovery. Like a mobile number, if your landline number ever changes, make sure to change it in your account recovery information.

Recovery codes. This is also less common, but doesn't suffer from issues relating to change. Some services let you generate one or more "recovery codes": random numbers that, in the event of password failure, can be used once to sign in to your account. The issue here is that you must create and save them somewhere secure so they're available when needed.

Secret questions. Some services still use them, but they should not. It's been shown that they're often guessable and significantly less secure. If you have a choice, use one of the alternatives above. If you have no choice, make sure you do not forget the answers to the questions you choose.[98]

[98] I used to be surprised at how often people forget their answers, but it makes an odd kind of sense. When setting up the account, they don't want to answer the questions or want to answer them extra-securely, so they enter nonsense. Later, when the account is important enough to need recovery, they can't remember the nonsense answers.

12 Steps to Keep from Getting Your Account Hacked

> *"My account has been hacked into several times. If I'm able to recover it, it just gets hacked again. Sometimes I can't recover it, and I have to start all over with a new account. What can I do to stop this all from happening?*

I don't get this question a lot, but I really wish I did. What I get instead, repeatedly, is "I've been hacked, please recover my account/password for me!" (Which, for the record, I cannot do, no matter how often or how nicely, or not so nicely, I'm asked.)

The only salvation is prevention, and this applies to email, social media, and pretty much any online account you have.

What can you do to make sure your account doesn't get hacked in the first place?

1: Select a good password

You'd be shocked at how easy many passwords are to guess. Your pet's name, your pet's name spelled backwards, your favorite TV character's catchphrase, your boyfriend or girlfriend's name (or "ilove" followed by that name), and so on.

If you think people can't guess it, **you are wrong**. They can and will.

"iLoveMikey" is a *bad* password. "j77AB#qC@^5FT9Da" is a great password. You can see the problem, though: great passwords are hard to remember.

So compromise.

- Avoid single or pairs of full English words or names unless you make a longer pass*phrase* of at least three and preferably four or more words.
- Include a mix of uppercase and lowercase letters and numbers.
- Make sure the password is at least 12 characters long, and ideally 16 or longer, if supported.

"Macintosh" is bad. "Mac7T0shB00k" (based on the easy-to-remember "Macintosh Book") might be good. "HondaPrelude" is bad, but "SilbrPre7ood6" (based on "Silver Prelude 6") might be ok.

Bottom line: pick a random-looking password YOU can remember but THEY would never guess… and assume that THEY are always really great guessers.

For more, see: What's a Good Password?[99]

[99] https://askleo.com/5440

2: Protect your password

A scenario I see much too often starts with "I thought I could trust my boyfriend/girlfriend/husband/wife/co-worker, so I gave them my password. Then we had an argument."

How much damage can someone do if they're angry with you and they have the password to your account? A lot.

It's simple: Trust no one. *I'm serious about this*. Your friends are your friends until one day they're not. Naturally, there are exceptions, but if there's the least bit of doubt, don't reveal your password. Especially if someone is pressuring you to do so.

For more, see: The Biggest Risk to Your Privacy.[100]

3: Set and protect your "secret answers"

It's fallen out of favor as not being particularly secure, but many systems still use a "secret question" and its answer as the key to account recovery or password reset. The problem is, many people choose secret answers nearly anyone can guess or easily find out.

However, *there's nothing that says your answer has to correspond to the question*. Instead, pick an answer that is unrelated to the question. Perhaps your city of birth should be Crayola, Chardonnay, or WindowsExplorer. Treat secret answers like another password. Make it long, obscure, completely unrelated to the "question", and impossible for someone else to guess.

As long as you can remember it when needed, it doesn't matter what it is.

For more, see: How to Choose Good Security Questions.[101]

4: Set (and maintain!) alternate email address(es)

Many services use one or more alternate email addresses to mail you a password recovery link if you forget yours. You must set this up **before** you need it.

First, *make sure to configure* that option using an email account on a different system. Create and use a Yahoo account for your Outlook.com alternate email, for example.

Second: *don't lose the alternate account*. For many systems, if you can't access that alternate email account, you cannot get your password back, and you will not be able to recover your primary account. Remember to log into that alternate account every so often to keep it from being shut down for inactivity.

I've seen too many cases where people lose their alternate email address or let the account lapse and then find themselves totally out of luck when they really need it to recover their primary account.

[100] https://askleo.com/27036
[101] https://askleo.com/4624

For more, see: Please Set Up and Maintain Account Recovery Information[102] in the next chapter.

5: Set (and maintain!) mobile or other telephone number(s)

This is very similar to an alternate email address, and can be used in place of one if you've configured it beforehand. Once again, you must set this up *before* you need it.[103]

If you can't access your account, the service will text you a recovery code. If you don't text or have a text-capable phone, some can call you with an automated voice recording of the recovery code. You then enter the code, proving you have access to the phone number that was previously configured as belonging to that account, and regain access.

Keep this number up to date! I regularly hear from people who've lost access to their accounts permanently because the phone number they originally configured[104] is no longer theirs.

Also, keep in mind that this number must be able to reach you where you are, and may even be triggered as an additional security measure if you travel outside of your normal area. If that's not possible, configure some other form of security, such as the alternate email mentioned above, or other techniques offered by your service provider.

For more, see: A One Step Way to Lose Your Account Forever.[105]

6: Enable two-factor authentication

Two-factor (or "multi-factor") authentication is the current holy grail when it comes to account security. **With two-factor properly enabled, hackers cannot get into your account *even if they know the password***.

The second factor that proves you are who you say you are is typically either:

- A mobile app that provides a random number on demand that you must provide when you log in
- A text message sent to a phone number you configure when you set up the account, which you then also enter at login

Once logged in, you can disable this requirement on machines you use frequently. Hackers are not able to provide the second factor, so they can't get in.

For more, see: Two-Factor Authentication Keeps the Hackers Out.[106]

---

[102] https://askleo.com/149957
[103] I often hear from folks who are concerned that providing a phone number is just another way to track you. I don't buy into that conspiracy theory. Providing a phone number is all about being able to prove you are the rightful account owner should you ever lose access to the account.
[104] https://askleo.com/15264
[105] https://askleo.com/15584
[106] https://askleo.com/16401

7: Other provider-specific techniques

Some providers have additional recovery techniques. For example, you can create a recovery code for your Microsoft account that you save somewhere safe and use to recover your account.

Look for options like these or others within the services you use regularly.

And remember, you must set them up before you need them.

For more, see: Recover Your Microsoft Account Later by Setting Up a Recovery Code NOW.[107]

8: Use a different password on every site

I've written about this extensively: it's important to use different passwords on each of your important sites.

The reason is simple: if a hacker manages to discover your password on one account, they will go try your username and password, or email and password, on a multitude of other services. If you used the same password on another service they happen to try, that account will quickly be hacked as well.

Password managers like 1Password, RoboForm, and others are excellent ways to maintain multiple, complex passwords for multiple sites without needing to remember them yourself.

For more, see: Why Is It Important to Have Different Passwords on Different Accounts?[108]

9: Use a password manager

I realize that "hard to guess" is at odds with "easy to remember" and both are at odds with not re-using passwords.

That's where password managers (also called vaults or safes) come in.

If you forget your password, or you forget the answer to your secret question, or lose access to your alternate email account, or somehow lose the ability to use any of the password recovery mechanisms provided by the service, well, to put it bluntly, you are SOL: severely out of luck.

Don't forget your own password. Don't forget the answer to your own secret question(s). If you must write your information down, keep it in a secure place. A sticky note on your monitor under your mouse pad or other easy-to-get-to place is not secure. Your wallet might be secure. A locked cabinet or safe might be secure. A properly encrypted file on your computer might be secure.

But remembering this information securely is exactly what password managers are designed to do for you.

[107] https://askleo.com/16142
[108] https://askleo.com/4931

For more, see: Are Password Managers Safe?[109]

10: Be skeptical

You should never be asked to email anyone your password.

Ever.

There are some very common phishing attempts that threaten you with account closure unless you respond to the email with information about your account (like your login name and password). Those emails are bogus. Mark them as spam and ignore them. Any email that requires you to respond with any information that includes your password is almost certainly a phishing scam.

Similarly, many phishing scams attempt to get you to click on a link to do something important relating to your account. Instead of taking you to the service, they take you to a fake page that looks like the service, but instead is a page designed to capture your username and password when you try to log in. If you have any doubt, don't click the link in the email. Instead, go to the service in question yourself, using your web browser. If there's something important, it'll almost certainly be presented there.

For more, see: Phishing: How to Know it When You See It.[110]

11: Remember that free services have little to no support

The vast majority of the account hacks I hear of — the hacks where people are ultimately unable to recover their accounts — involve free services with little to no support.

There may be a knowledge base or a peer-to-peer support forum, but there is rarely someone to email and almost never someone to call.

You are responsible for your own account security.

It's often true, and certainly safest to assume, that no one will help you should something go wrong. That means it's up to you to take the preventative measures I've outlined as well as keep your information up to date as things change.

For more, see: Are Free Email Services Worth It?[111]

12: Learn from your mistakes

Finally, if you realize that:

- The answers to your secret questions are obvious, or
- You no longer have access to your alternate email address or never set one up, or
- You no longer have access to your old mobile number or never set one up, or

[109] https://askleo.com/5555
[110] https://askleo.com/16491
[111] https://askleo.com/2217

- Your passwords are short and just plain lame, and you use the same one everywhere…

Fix it NOW! Before it's too late.

Trust me: if you get hacked and it's for one of those reasons, or you lose access to your hacked account because you didn't bother to prepare, you'll kick yourself.

And you may very well lose access to that account and all its data forever.

Is Using the Cloud Safe?

One of the comments I received on my article on lessons learned from a fairly public online hacking[112] was very concise:

"That's why the cloud is dangerous."

I think a lot of people feel that to varying degrees.

I strongly disagree.

I also think believing the cloud is dangerous prevents you from taking advantage of the things that the cloud can do for you—things like protecting your data.

It also misses the point that there are a number of things you're already doing things "in the cloud" safely, and have been *for years*.

What is "the cloud"?

I have to start by throwing away this silly, silly term, "the cloud." It's nothing more than a fancy marketing term. Ultimately, it has no real meaning.

The cloud is nothing more than services provided online over the internet.

Seriously, that's all it is.

Another way I saw it expressed recently was, "'The cloud' is simply using someone else's computer."

Be it services that provide a place to store your data, enable you to communicate with others, provide applications, sell you things, or answer your technical questions, it's all happening in the cloud.

That's nothing new.

The cloud is new in name only

You've probably been using online services long before anyone thought to slap the name *cloud* on 'em.

- Do you have an online email account like Outlook.com or Gmail? You're keeping your email in the cloud.
- Do you use any kind of email? It gets from point "A" to point "B" through the cloud.
- Do you upload pictures to a photo-sharing site like Flickr, Picasa, or Photobucket? That's the cloud.
- Do you use any social media? Yup, they're in the cloud too.

[112] https://askleo.com/103465

- Do you use an online backup service? You've been backing up to the cloud.

You get the idea.

I really, really want to drive home the point that this thing people are calling *the cloud* is nothing new. You've been using it already—probably for years before that silly name was attached to it.

So let's jettison the name and all the baggage comes with it, and call it what it really is: online services.

OK, fine. But is the cloud dangerous?

No more so now than it's ever been.

In fact, I'll claim that the average online service is becoming *safer* than ever before as service providers learn from mistakes and implement industry best practices.[113]

If anything has changed at all, it's the breadth of available online services and the number of people using them.

The fact is that any tool, when misused, can be dangerous.

For example, placing sensitive information in your online email account (and *only* your online email account), and then not using proper security on that account, is *absolutely* dangerous, and always has been. It's not that online email accounts are dangerous. The danger arises from *using them improperly*.

The same is true for any online service, be it those generating the latest buzz or those you've been using for years.

We're all at the mercy of service providers

At this point, many folks point out that the security breaches that we hear about are often the fault of, or related to, a problem at the provider of the service in question.

Many are, it's true.

---

[113] I don't have the data to back it up, but my feeling, based on being in this industry for as long as I have, is that by and large, service providers are getting better. The state of the art in online security is improving overall. If it seems like problems are happening more often, my sense is that it's simply because there are more online services now than there ever have been. My gut tells me that the number of failings as a percentage of available online services is going down.

But you know what? *That's not new either*.

As long as there have been service providers, there have been mistakes, breaches, and policy screw-ups at service providers.

I'm not (not! not! not!) trying to excuse service providers for making mistakes or screwing up. Every fiber of their corporate being should be working to prevent security-related errors, and mitigate the impact when they happen.

But the reality we have to accept is that ultimately, service providers are staffed by humans, and humans make mistakes. Saying mistakes should never happen is unrealistic.

And it's extremely poor security planning.

Besides, when it comes to security issues, we are most often our own worst enemies.

No one can protect you from you

Let's go back to the Mat Honan hack[114] for a moment, which is where the "the cloud is dangerous" comment originated.

Mat didn't lose his data because of the breaches he experienced.

Mat didn't lose his data because of problems with the online services (though there definitely were issues).

He lost his data because *he wasn't backed up*. Even if he had not been hacked, he was at high risk of losing everything anyway had he lost his laptop or experienced a simple hard disk failure.

Had he been backing up his data, I'm betting there wouldn't have even been a news story.

On top of that, the hack reached as many of his accounts as it did because *he had linked all of his accounts together*. Mat helped the hackers get to his accounts.

No, the lesson here isn't that online services are dangerous. The lesson here is that *we have to assume responsibility for our own safety*.

And I'll say it once again: this is not new.

How to use online services safely

Using online services safely really boils down to not much more than the guidelines we've all heard before.

All, of course, augmented by a dose of common sense.

- Back up. If it's only in one place, it's not backed up.

[114] https://askleo.com/103465

- Use strong passwords, and set up and *keep current* all account recovery information.[115] Use extra security, such as two-factor authentication if supported.
- Encrypt[116] sensitive data stored online.
- Understand the security ramifications of using someone else's computer, or someone else using yours.
- Understand how to use internet connections provided by others securely, especially open Wi-Fi hotspots.[117]
- Don't link your important accounts together in such a way that breaching one opens the door to all of them; use different passwords[118] (and perhaps even different email addresses) for each.
- Keep your software up to date, scan for malware, and do all the other items commonly listed to keep your computer safe on the internet.[119]

Only the part about using different email addresses for different accounts is relatively new—everything else should sound really, really familiar.

It really can be safe

To be clear, there's no such thing as perfect security,[120] and that's true whether you keep your information securely locked away only on your own computer in your bedroom, or if you store it in the cloud. There's always something that can go wrong.

But by following basic security guidelines, there's no reason that most of the popular online services can't be used safely—at least as safely as the services you're already using.

Used properly, they even *add* security by providing things like additional backups, throw-away email accounts, data replication, and more.

You do have to assume responsibility for your own security, and that includes taking reasonable precautions to prevent a problem and taking additional steps to minimize the impact should an issue arise.

Yes, you can avoid online services all together (just remember that means walking away from email as well), but you'd be missing out on so many of the opportunities the internet has to offer.

Rather than asking "Is the cloud dangerous?", learn to use it safely. You'll be much better off for it.

I know I am.

[115] https://askleo.com/15584
[116] https://askleo.com/43770
[117] https://askleo.com/4790
[118] https://askleo.com/11788
[119] https://askleo.com/2374
[120] https://askleo.com/21748

Postscript

Mat Honan, the victim of that public hacking I mentioned at the beginning, published an update detailing how he's recovered from his hacking.

One relevant quote that struck me: "I'm a bigger believer in cloud services than ever before."

This is the gentleman whose experience initiated this very discussion. While others are quick to blame "the cloud", after all is said and done, he's not one of them.

Neither am I.

Find his story at Mat Honan: How I Resurrected My Digital Life After an Epic Hacking.[121]

[121] https://go.askleo.com/honanrecovery

How Long Should a Password Be?

For a long time, the common thinking was that the best, most practical passwords consisted of a random combination of upper and lower-case letters, numbers, and a special character or two. If so composed, password length needed to be only eight characters.

Randomness remains important, but as it turns out, size matters more.

Large-scale account hacks

When you hear about large numbers of accounts being stolen by a hack at some service provider, you are naturally concerned that the hacker may now have access to your account names and passwords. If the service was storing your *actual* passwords, that could indeed be the case. (If a service is storing your *actual* passwords,[122] they simply don't understand security or they have made some horrifically bad decisions.)

In fact, most services store[123] an encrypted (technically, a "hashed") form of your password. For example, if my password were "password" (and that's a very poor password, of course), then a service might store

5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

As the hash value that corresponds to that password. [124]

What that means is that hackers do *not* get a list of usernames and passwords. What they get is a list of usernames and password *hashes*.

And what's great about hashes is that you can calculate a hash from a password, but you cannot do the reverse—*you cannot calculate the password from the hash*.

As a result, one would think that by being hashed it'd be pretty unhackable, right?

Sadly, not so much.

Dictionary attacks

The most common type of password attack is simply a high-speed guessing game. This doesn't work on an actual log-in page;[125] they're slow and deny further access after too many failed attempts. But this technique works wonderfully if the hacker has the entire database of account and password hashes sitting on his computer.

---

[122] If they can respond to an "I forgot my password" request with your *actual, current* password, then they have stored your password. This is bad. Best practice is to reset it to something new, either via a reset link, or by emailing a new password to you *exactly once*, after which the service no longer has it.
[123] https://askleo.com/136163
[124] For the curious, I'm using an un-salted sha256 as the hashing function here. That's technically better than md5 or sha1 that's commonly used.
[125] https://askleo.com/14547

These attacks involve starting with an exhaustive list of possible words and known common passwords (including names, profanities, acronyms, and more) and perhaps a few rules to try interesting and common ways that people try to obfuscate words. They calculate the hash of each guess, and if it matches what was found in the compromised database of account information that they're working against, they've figured out the password for that account.

As we'll see in a moment, it's easy for hackers to make an amazing number of guesses is a short amount of time.

That's why you're not using a short password or common obfuscations, right?

That's why a password created from a totally random combination of characters is best. It forces hackers to move on to a true brute force attack of every possible combination to gain access.

Brute force attacks

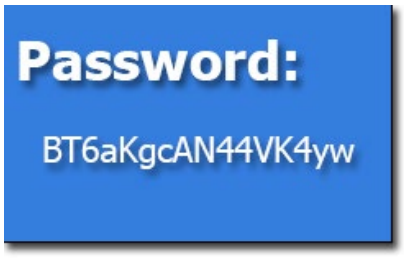
Computers are fast. In fact, the computer on your desk is so fast that its ability to do simple operations is measured in terms of *billions* of operations per second.

Creating a password hash is not a simple operation, on purpose. However, it's still something that can be done very quickly on most machines today. Spread the work over a number of machines—perhaps a botnet—and the amount of processing power that can be thrown at password cracking is amazing.

The net impact is that it's now feasible to calculate the encrypted hash values for *all possible eight-character passwords* comprised of upper and lowercase alphabetic characters and digits.

Sixty-two possible characters (26 lower case, 26 upper case, 10 digits), in each of the eight positions gives us 221,919,451,578,090,[126] or over 221 trillion, combinations.[127]

This seems like a lot, until you realize that an off-line attack (which is easily performed once you've stolen a database of usernames and encrypted passwords) can be completed in a few hours. (This assumes technology which can "guess" something like 10 billion passwords per second—which, for those performing these kinds of attacks, is quite possible.)



It doesn't matter what your password is; if it's eight characters using upper and lowercase letters and numbers, the hackers now have it—even if it was well hashed by the service they stole it from.

[126] OK, OK. Technically, the number is actually 221,919,451,578,090 + 3,579,345,993,194 + 57,731,386,986 + 931,151,402 + 15,018,570 + 242,234 + 3,844 + 62. Then we also add in the possibilities of seven-character passwords, six, five, four, and so on. I'm not doing the math. It's around 225 trillion.

[127] Many of the numbers and attack estimates here come from or are based on GRC.com's excellent Password Haystack page. Included there are links to an excellent *Security Now!* podcast discussing password length and how size really does matter.

Why 12 is better and 16 better still

As we've seen, eight-character passwords give you over 221 trillion combinations, which can be reasonably brute-force guessed offline in hours.

Twelve characters give you over three sextillion (3,279,156,381,453,603,096,810). The offline brute-force guessing time in this case would be measured in *centuries*.

Sixteen takes the calculation off the chart.

That's why 16 is better than 12, and both are better than eight.

What about special characters?

I left out special characters.

Let's say that the system you're using allows you to use any of 10 different "special characters" in addition to A-Z, a-z, and 0-9. Now, instead of 62 characters, we have 72 possibilities per position.

That takes us to 700 trillion possibilities for an eight-character password.

Compared to sticking with the original 62 letters and numbers, adding only a single “normal” character makes a nine-character password significantly more secure.

That takes us to over 13 *quadrillion* possibilities.

Yes, adding special characters makes your password better, but significantly better *yet* is simply to add one more character.

So add two. Or six. ☺

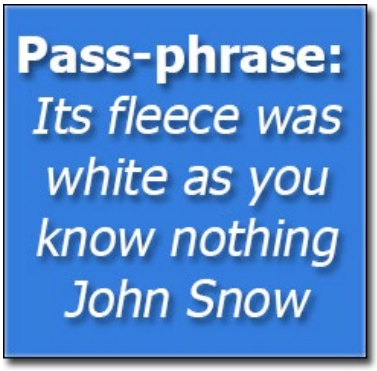
Long passwords are good; passphrases are better

The difference is really a semantic one, but in general:

- A password is a random string of characters.
- A passphrase is a longer string of words.

Why pass*phrase*? Because they're easier to remember, so it’s easier to make longs—and as we saw, password length is perhaps the single easiest way to increase the security of a password.

"BT6aKgcAN44VK4yw" is a very nice, secure 16-character password that's difficult to remember. In fact, the only way to use this is with a password manager that remembers it for you.



On the other hand, "Its fleece was white as you know nothing John Snow", at 50 characters, is wonderfully long, secure, and most of all, *memorable*. Much like the now-canonical example of "Correct Horse Battery Staple", you may even have a difficult time forgetting it.[128]

The biggest problem with passphrases? Many services that use passwords don't allow spaces or such lengthy passwords.

Shouldn't services fix this and do better?

Absolutely, they should. And many do.

As I've stated above, passwords shouldn't be kept in plain text anywhere by the service at all, yet some do.

There are techniques that make brute-force attacks significantly harder, yet many use techniques that are *easier* than the example above.

There are services that do a great job of keeping your information secure. There are also services that don't. The problem is that you really can't be certain which is which.

To be safe, you have to act like they're all at risk.

The bottom line

The bottom line for staying safe is simply this:

- *Don't trust that the service* you're using is handling passwords properly. While many do, it's painfully clear that many do not, and you won't know which kind you're dealing with until it's too late.
- *Use longer passwords*: 12 characters minimum and 16 if at all possible.
- *Use even longer passphrases* where they're supported or where information is particularly sensitive.
- *Use a different password* for each different site login you have. That way, a password compromised on one service won't give hackers access to everything else.[129]

Even the best eight-character passwords should no longer be considered secure. Twelve is "good enough for now," but consider moving to 16 for the long run.

[128] Particularly if you're a *Game of Thrones* fan. ☺ And yes, I know that John Snow is actually Jon Snow. That's another level of handy, yet easy to remember, obfuscation.
[129] https://askleo.com/11788

Why Is It Important to Have Different Passwords on Different Accounts?

> *"Is it safe to have the same password for all of my email accounts? If one has an account in Yahoo! mail, Gmail, Rediff mail, etc., and sets the same password for all of them, will it be easier for a hacker or phisher to find out about it?*

Using different passwords is much safer than using one password everywhere. In fact, it's critical.

Why?

Because hackers know that most people have more than one account and that most people don't take the trouble to set different passwords.

Admit it, you're lazy

I'll admit it: I'm lazy. When it comes to managing passwords, I'll bet money that most people are.

One password everywhere is *so much easier*. It's easier than even the easiest password management system.

It simplifies our lives not to have to remember passwords or use any special tools to remember for us.

The problem is, it makes hackers' lives easier, too.

Hackers know we're lazy

Hackers know that people find it easier to have one password everywhere.

Hackers know that people generally have more than one account.

Hacking a single account acts as a foot in the door to the others and leads to all sorts of mayhem.

One account leads to more

It's easy to guess that if a person logs in with username X and password Y on a system like Yahoo! mail, it's likely they'll replicate both username X and password Y on other services.

Once they've breached one account, hackers get clues that let them access other accounts.

Account confirmations and notifications are frequently sent via email. What that means is that your hacked email account contains many clues as to what other accounts you have.

If you use the same password everywhere, it's easy sailing for the hacker to quickly try those out and log in as you at multiple services.

For example, your Facebook login is your email address and a password. Well, if they've hacked your email account and you use the same password everywhere, they now know how to log in as you on Facebook.

The hack might not be your fault

Hacks happen through no fault of your own. You could be maintaining perfect security and still end up compromised.

Consider all the places you have online accounts. Let's assume that the one with the poorest security gets hacked, and the contents of their entire username/password database is stolen.

You just got hacked, and it wasn't your fault.

However: if you're using one password everywhere, the hackers now know it.

There can't be only one

The bottom line is that using one password everywhere is a risk you shouldn't take.

At a minimum, use unique passwords for your important accounts, like banking and other financially related activities *and email*.

All of your email accounts are important, particularly if they can be used for password recovery on other accounts. All a hacker needs to do is hack your email account and then run over to some other account and request a password reset to be emailed to the email account they now control.

Managing lots of passwords

Whenever I talk about giving each login a different, strong password, people strongly object. "No way am I going to remember all those passwords, especially if you're going to insist that they're complex on top of everything else."

You don't have to.

For example, I don't know my online banking password. Who's going to remember something like yFK86jk8q45B? (And no, that's not it. I said something like that.)

Yet I use my account frequently.

Let your computer do the remembering for you.

I'm a big fan of password management programs, in particular 1Password.[130]

[130] https://askleo.com/152844

It creates a secure database of your login IDs and passwords and stores them so that only you can get at them with your single, master password. (And yes, that password needs to be strong and memorable.)

Password vaults ease the entire process of logging in by filling in the user ID and password for you; you don't even need to know what they are.

They use strong encryption to keep your password database secure on your machine(s) and support synchronizing or accessing that database across multiple machines and mobile devices.

And they enable you to use different and strong passwords on every single site.

Why Password Managers are Safer than the Alternatives

> *"Recently I tried to use RoboForm for an account at a large financial institution, but I couldn't get it to work. In response to my inquiry, this institution said they do not permit log in using credentials that are stored on software because the security of the password could become jeopardized if my computer were hacked, invaded, etc. Is this true? Am I safer not to use tools like RoboForm?*

There are people who believe that using password managers represents a single point of failure. Very technically, they are correct: if someone gains access to your password manager, they have access to everything within it.

Not so technically, I strongly believe they are misguided. Using a password manager is, in my opinion, *significantly* safer than the alternatives.

Security best practices

Password security demands that you:

- Have good, strong passwords (long and complex).
- Keep them nowhere but in your head (memorable).
- Use a different password on every site or service (unique).

Yes, indeed, that would be ideal.

Without using a password manager, it's also completely impractical. Those requirements simply can't all be met at the same time. At least one, if not two, will be compromised without the aid of a password vault.

Without a password manager

Without a password manager, you'll compromise your security in some way.

- You'll choose a less secure, easy-to-remember password (short and/or not complex).
- You'll use the same password at multiple sites (not unique).
- You'll save the password using technology that is not secure (not memorable).

Any one of those can significantly compromise your security.

With a password manager

Password managers make best practices trivially easy. Using a password manager allows you to:

- Generate and use secure, complex, and appropriately long passwords.
- Never need to type or remember passwords—the password manager remembers them for you.
- Use different passwords on different sites.

These are things that people *don't* do unless they have a tool in place to help them. Password managers are specifically designed to do exactly that securely.

Most password managers add several features that make improved security even more convenient. They can:

- Synchronize your information across multiple computers.
- Be used on mobile devices.
- Automatically fill in not just passwords, but common web forms.
- Securely store other information of many types.

And they do all of that with more security than almost all alternatives.

If you're compromised, you're compromised

It is true that if your computer is compromised, all bets are off. Malware *could* gain access to whatever it is you have stored on the computer.

For example, while I'm logged into 1Password, all the information is technically available to software running on my machine—good software or bad.

That's a serious concern, and not to be taken lightly.

But it's a concern that exists *regardless of whether you use a password manager or not*. All bets are off if a keylogger captures what you enter when you log in to your bank account.

Avoiding a password manager doesn't increase your security one whit.

But are password managers safe?

Yes. Password managers are safer than any practical alternative.

There are no absolutes -- that, too, is a practical reality. There is no such thing as absolute security.[131] As I said earlier, if you fall victim to malware, all bets are off, no matter what technique(s) you use.

Password managers are the safest way to keep a record of your online account information, but they are no safer than:

- The master password you use to access the password manager.
- Your own ability to use your computer safely.[132]

The last one scares most people, but my claim is that using password managers is, in fact, one way to use your computer more safely.

What I do

I keep my machine(s) secure by doing the traditional things that you hear over and over:[133] keeping software up-to-date, running up-to-date scans, avoiding malicious websites and downloads, not falling for phishing, and so on and so on.

I use 1Password[134] to manage my passwords and additional security information.

I use Google Authenticator, a form of two-factor authentication, to access my 1Password vault. You can't get in to my 1Password account *even if you know my master password*. To get access to my 1Password vault, you need both my master password *and* my mobile phone.

I have 1Password automatically log out after some amount of time on any device which I'm not 100% certain won't get stolen or accessed without my permission.

I keep my master password secure and complex.[135]

I back up my 1Password vault regularly.

I'm not going to claim it's impossible for anything bad to happen -- that'd be a foolish claim. I am, however, very satisfied with the risks and trade-offs, and absolutely convinced that using a password manager keeps me as safe as possible — and safer than not using one at all.

Let's face it: even doing business *offline* has risks and trade-offs.

[131] https://askleo.com/16029
[132] https://askleo.com/2374
[133] https://askleo.com/2374
[134] https://askleo.com/152844
[135] https://askleo.com/5440

My Email Got Hacked. How Do I Fix It?

It seems like not a day goes by when I don't get a question from someone that boils down to their email account having been hacked.

Someone, somewhere, has gained access to their account and is using it to send spam, access other online accounts, hassle contacts, and more. Sometimes passwords are changed, sometimes not. Sometimes traces are left, sometimes not. Sometimes everything in the account is erased—including contacts and saved email—and sometimes not.

If that's happening to you, your email account has been hacked.

Here's what to do next if it happens to you.

1. Recover your account

Log in to your email account via your provider's website.

If you can log in successfully, consider yourself *extremely* lucky, and proceed to Step 2 right away.

If you can't log in, even though you're sure you're using the right password,[136] then the hacker has probably changed your password. *The password you know is no longer the correct password*.

You must then use the "I forgot my password" or other account recovery options offered by the service.

This usually means the service will send password-reset instructions to an alternate email address that you do have access to, or send a text message to a mobile phone number set up previously.

If the recovery methods don't work—because the hacker changed everything, or because you no longer have access to the old alternate email or phone—then you may be out of luck.[137]

If recovery options don't work for whatever reason, your only recourse is to use the customer service phone numbers or email addresses provided by that email service. For free email accounts, *there is usually no customer service*. Your options are generally limited to self-service recovery forms, knowledge base articles, and official discussion forums where service representatives may (or may not) participate. For paid accounts, there are typically additional customer service options that are more likely to be able to help.

[136] https://askleo.com/15079
[137] https://askleo.com/15584

Important: If you cannot recover access to your account, *it is now someone else's account*. I can't stress this enough. It is now the hacker's account. Unless you've backed up, everything in it is gone forever, and you can skip to Step 5. You'll need to set up a new account from scratch and start over.

2. Change your password

Once you regain access to your account (or if you never lost it), *immediately* change your password.

As always, make sure that it's a good password:[138] easy to remember, difficult to guess, and long. In fact, the longer the better,[139] but make sure your new password is at least 16 characters or more—ideally 12 or more, if the service supports it. See How Long Should a Password Be? for more information.

But don't stop there.

Changing your password is not enough.[140]

3. Change or confirm your recovery information

While a hacker has access to your account, they might leave your password alone so that you won't notice the hack for a while longer.

But whether they change your password or not, they may change *all of the recovery information.*

The reason is simple: if you change your password, the hacker can follow the "I forgot my password" steps and they can reset the password out from underneath you using the recovery information *they* set.

Thus, you need to check all of it and change much of it right away.

- **Change the answers to your secret questions** if your account uses them. They don't have to match the questions (you might say your mother's maiden name is "Microsoft", for example); all that matters is that the answers you give during a future account recovery match the answers you set today.
- **Check the alternate email address(es)** associated with your account and remove any you don't recognize. The hacker could have added his or her own. Make sure you have alternate email addresses configured and that they are accounts that belong to you that you can access. I really can't emphasize that last point enough: the number of accounts that are lost because folks could not access the recovery email address is amazing.
- **Check any phone numbers associated with the account.**[141] The hacker could have set their own. Remove any you don't recognize. Make sure that if you provide a phone number, it's yours and no one else's, and you have access to it. As with alternate email addresses, I

[138] https://askleo.com/5440
[139] https://askleo.com/4844
[140] https://askleo.com/15053
[141] https://askleo.com/15264

> really can't emphasize the last point enough: the number of accounts that are lost because people could not access the recovery mobile number is scary.

These are the major items, but some email services have additional information they use for account recovery. Take the time *now* to research what that information might be. If it's something a hacker could have altered, change it to something else appropriate for you.

Overlooking information used for account recovery allows the hacker to easily hack back in. Make sure you take the time to carefully check and reset all as appropriate.

It's a simple trap too many people fall into causing them to lose their email account forever. Check out A One-step Way to Lose Your Account Forever.[142]

4. Set up two-factor authentication

If you don't have it enabled on your account already, now is the time to enable two-factor authentication.

Why? Because if you had enabled it, you wouldn't be here. Two-factor authentication means that even if hackers discover your password, they still can't sign in. They don't have the second factor — your phone, an authentication app, access to a specific email address, etc. — that only you do. Without that access, they simply can't get in.

And don't let the hype about SMS being less than secure stop you, if that's your only option. It's more than secure enough for the average user, and it's still better than no two-factor authentication[143] at all.

5. Check "out of office" messages, reply-to, forwards, and signatures

If your email service provides an out-of-office or vacation-autoresponder feature, or some kind of automatic signature that appears at the bottom of every email you send, it's possible people already know you're hacked.

Hackers often set an autoresponder in a hacked account to automatically reply with their spam. Each time someone emails you, they get this fake message in return, often written so it sounds like you sent it.

If your account includes the ability to set a different "Reply-To:" email address, make sure that hasn't been set. Hackers can set this so individuals who think they're replying to you end up replying to the hacker instead.

Make sure your email is not being automatically forwarded to another email address. If it's available, hackers often set this option to receive copies of every email you get. They can use this to break into your account again even after you recover it.

[142] https://askleo.com/15584
[143] https://askleo.com/70786

Check any signature feature the service supports. Hackers often set up a signature so that every email you send includes whatever they're promoting, including a link to a malicious web site.

6. Check related accounts

This is perhaps the scariest and most time-consuming aspect of account recovery. The risks are high, so understanding this is important.

While the hacker has access to your account, they have access to your email, including past and current emails as well as what arrives in the future.

Let's say the hacker sees you have a notification email from your Facebook account. The hacker now knows you have a Facebook account, and the email address you use for it. The hacker can go to Facebook, enter your email address, and request a password reset.

A password reset sent to your email account—which the hacker has access to.

As a result, the hacker can now hack your Facebook account by virtue of having hacked your email account.

In fact, the hacker can now gain access to any account associated with the hacked email account.

Like your bank. Or PayPal.

Let me say that again: *because the hacker has access to your email account, he or she can request a password reset be sent to it* from any other account for which you use this email address. In doing so, the hacker can hack and gain access to those accounts.

What you need to do: check your other accounts for password resets you did not initiate and any other suspicious activity.

If there's *any* doubt, consider changing the passwords on all those accounts as well. (There's a very strong argument for checking or changing the recovery information for these accounts, just as you checked on your email account, for all the same reasons.)

7. Let your contacts know

Some disagree with me, but I recommend letting your contacts know that your account was hacked, either from the account once you've recovered it, or from your new email account.

Inform all the contacts in the online account's address book; that's the address book the hacker had access to.

I believe it's important to notify your contacts so they know not to pay attention to email sent while the account was hacked. Occasionally, hackers try to impersonate you to extort money from your contacts. The sooner you let them know the account was hacked, the sooner they'll know that any

such request—or even the more traditional spam that might have come from your account—is bogus.

8. Start backing up

A common reaction to my recommendation that you let your contacts know is: "But my contacts are gone! The hacker erased them all, and all of my email as well!"

Yep. That happens.

It's often part of a hacker not wanting to leave a trail—they delete everything they've done, along with everything you have. Or had.

If you're like most people, you've not been backing up your online email. All I can suggest at this point is to see if your email service will restore it for you. *In general, they will not.* Because the deletion was not their doing, but rather the doing of someone logged into the account, they may simply claim it's your responsibility.

Hard as it is to hear, they're absolutely right.

Start backing up your email now. Start backing up your contacts now.

For email, that can be anything from setting up a PC to periodically download the email, to setting up an automatic forward of all incoming email to a different account, if your provider supports that. For contacts, it could be setting up a remote contact utility (relatively rare, I'm afraid) to mirror your contacts on your PC, or periodically exporting your contacts and downloading them, which is what I do.

9. Learn from the experience

Aside from "you should have been backing up," one of the most important lessons to learn from this experience is to consider all of the ways your account could have been hacked, and then take appropriate steps to protect yourself from a repeat occurrence in the future.

- Use strong passwords that can't be guessed, and don't share them with *anyone*.
- Use a password manager.
- Use two-factor authentication.[144]
- Don't fall for email phishing attempts. If they ask for your password, they are bogus.[145]
- Don't click on links in email that you are not *100%* certain of. Many phishing attempts lead you to bogus sites that ask you to log in, and then steal your password when you try.
- If you're using WiFi hotspots, learn to use them safely.[146]
- Keep the operating system and other software on your machine up-to-date, and run up-to-date security software.[147]

[144] https://askleo.com/16401
[145] https://askleo.com/3863
[146] https://askleo.com/4790
[147] https://askleo.com/3517

- Learn to use the internet safely.[148]

If you are fortunate enough to be able to identify exactly how your password was compromised (it's not common), then absolutely take measures so that it never happens again.

10. If you're not sure, get help

If the steps above seem too daunting or confusing, then definitely get help. Find someone who can help you get out of the situation by working through the steps above.

While you're at it, find someone who can help you set up a more secure system for your email, and advise you on the steps you need to take to prevent this from happening again.

Then follow those steps.

The reality is that you and I are ultimately responsible for our own security. That means taking the time to learn, and setting things up securely.

Yes, additional security can be seen as an inconvenience. In my opinion, dealing with a hacked email account is *significantly more* inconvenient, and occasionally downright dangerous. It's worth the trouble to do things right.

If that's still too much... well, expect your account to get hacked again.

11. Share this article

As I said, email account theft is rampant.

Share this article with friends and family. Statistically, one of you will soon encounter someone whose account has been hacked and will need this information.

Addendum: Is it my computer or not?

When faced with this situation, many people worry that malware on their computer is responsible.

That is *rarely* the case.

In the vast majority of these situations, your computer was never involved.

The problem is not on your computer. The problem is simply that someone else knows your password and has logged into your account. They could be on the other side of the planet, far from you and your computer (and often, they are).

Yes, it's possible that a keylogger was used to capture your password. Yes, it's possible that your PC was used improperly at an open WiFi hotspot.[149] So, yes, absolutely, scan it for malware and use it

[148] https://askleo.com/3517
[149] https://askleo.com/4790

safely, but don't think for a moment that once you're malware free, you've resolved the problem. *You have not.*

You need to follow the steps outlined here to regain access to your account and protect it from further compromise.

You'll use your computer, but your computer is not the problem.

Part 6: Protect Your Privacy

You're Just Not That Interesting (Except When You Are): Pragmatic Privacy

Privacy is a huge and controversial topic. So huge I can't tell you what steps to take, what settings to change, what apps to avoid, or what services to choose. Not only are there seemingly infinite options, but the options keep changing.

There are also about as many opinions on the topic as there are internet users. Anything I say is just one more voice in the crowd… but that's not going to stop me.

Let's take a pragmatic look at your privacy and your options.

Two kinds of privacy

"Privacy" is a really big term, so I want to define two types.

Implicit privacy is the privacy we assume when we use online services, operating systems, applications, and programs to manage our personal information and activities. Each has a set of rules -- often some formal privacy policy -- controlling their access to your information and what they do with it.

Explicit privacy is the privacy we control more directly with our choices. For example, choosing not to share a photo on social media is one form of explicit privacy. Keeping our passwords to ourselves is another. So are the settings we use to control who is allowed to see what we post.

The biggest difference between implicit and explicit privacy, in my mind, is the amount of control we have over it. We *implicitly* trust that the software and services will do as they say. We *explicitly* decide what to share based on what we believe may happen.

Privacy, policies, and Big Brother

Privacy -- or lack thereof -- when using popular services or software is big topic of discussion. For example, Window's tracking activity generates a great deal of concern. It's debatable whether the concern is warranted.

Any online service involves some amount of tracking. Visiting a simple website—even Ask Leo!— results in some amount of what might be considered tracking, usually in relation to advertising displayed on the site. Some consider that an invasion of privacy. The most common visible signs are advertisements that appear to follow you[150] from site to site as you browse the web.

[150] https://askleo.com/5670

All online services and websites have the ability to collect vast amounts of data derived from their users. Similarly, any and all software you install has the ability to collect usage information.

Whether or not you believe Big Brother is watching, the technology is there should he want to.

The (poor) choices we make

At the other end of the privacy spectrum are the (often poor) choices we make about what we share and with whom.

I often hear from individuals who've shared a password with a trusted friend only to be surprised when their privacy is violated because the trust was misplaced.

We've all heard stories of individuals losing jobs or job opportunities because of statements, photos, or videos posted on social media. Call your boss names on Twitter, for example, and there's no one to blame but yourself when you're shown the door the next morning. Have you posted "funny" pictures of yourself after imbibing a tad too much alcohol? That could be the reason you don't get the next job or loan you apply for.

When it comes to privacy, we're often our own worst enemy.

You're just not that interesting

I say it often: you and I just aren't that interesting as individuals. That your operating system might track what you do is pretty meaningless in terms of personal privacy. That advertisers might use what websites you visit and things you click on to tailor the ads you see is pretty benign.

The companies collecting this data aren't looking at you as an individual. They're looking for *trends* from the data of millions of users to determine what's being acted on, what's influencing the crowd, and what they might do better.

I do it, too. For example, do I care that you, specifically, looked at my newsletter? At a personal level I do, but I'm not going to sift through information on nearly 50,000 subscribers to see who did and who didn't. On the other hand, if 10,000 fewer people open the newsletter one week, that's information I want to be able to act on. I can only do that by tracking the behavior of 50,000 individuals in aggregate.

The same is true for most any company. Your personal privacy isn't being violated because nobody is looking at you specifically. One person just isn't that interesting; thousands or millions, on the other hand, almost certainly are.

But you might be interesting someday

There are two cases in which you might become interesting.

If you run afoul of the law. This isn't an issue for most. But if you live in an oppressive regime or are subject to investigation for your activities, it could be. Even this falls into two sub-categories: the unduly paranoid (a larger number of people than we might hope), and the legitimately concerned, for both legal and illegal reasons.

It is important to realize that if you fall into this category, law enforcement may have the right to collect information about you. This can include things we might brush off as irrelevant — like ad or service usage collected by your ISP or the services and software you use. I have to say law enforcement may have the right, because laws differ dramatically depending on where you live. Of more practical import, perhaps, law enforcement capabilities vary dramatically, based on everything from expertise to budget to jurisdiction to prioritization of limited resources.

Future opportunities. Some years from now, perhaps someone will research your history as part of a job application or something else where your record and reputation are important. What you post today, publicly or even privately, may influence their opinion tomorrow.

It's all so scary. What to do?

It'd be easy to read that last section, throw up your hands, and crawl into a hole, thinking privacy is a thing of the past -- at least when it comes to the internet.

If you're a criminal, you probably should be concerned. The only thing preventing you from being exposed is the limited resources of the law enforcement agencies who really do care about you specifically. There are steps you can take, but I'm not the one to help you take them.

For the rest of us living more mundane lives, my advice is pretty simple.

First, stop worrying about being tracked by the companies providing the services you use. They don't care about you as an individual. There is plenty of room for policy debate about what kinds of information they should and should not collect and how they should or should not use it, but in my opinion, that has little chance of impacting you *as an individual*.[151]

Second, don't post anything you wouldn't want made public. Learn the privacy policies and settings of your social media and other applications, and change them and/or change your behavior accordingly. Public once is public forever; there's no calling it back from the internet.

Think twice about what you post privately as well, since you're assuming your private audience won't someday make it public without your approval. This includes social media, but also things you share in any form, be it email, text messaging, or other media. We've all seen situations where communications once thought private were made public to great embarrassment or worse.

Privacy remains your responsibility

I remain a strong believer in our wonderfully interconnected world and all the opportunities it presents.

Naturally, it brings risk as well as reward.

[151] And if you're going to worry, then be more consistent. It's funny to me to get rants about the alleged privacy violations of company G, sent via an email address provided by company M, whose activity is on par with G. If the behaviors of the major service providers concern you that much, I know of no solution other than walking away from the internet entirely.

Ultimately, it's *our* responsibility to be aware of those risks, educate ourselves about the possibilities as well as the practical realities, and make careful choices accordingly.

Endnotes

Afterword

I hope this book helps you protect yourself against all the nasty things that happen to you in our internet-connected world.

If you find what you believe to be an error in this book, please register your book (the details are in an upcoming section) and then visit the errata page for this book. That page will list all known errors and corrections, and give you a place to report anything you've found that isn't already listed.

Register Your Book!

I've got additional updates, errata, and other bonus materials for you:

- *Updates For Life* to this book, as they're released.
- Downloads of this book in any or all of three digital formats:
  - PDF (for your computer or any device that can view PDF files)
  - .mobi (ideal for the Amazon Kindle), or
  - .epub (for a variety of other electronic reading devices).
- Other bonuses and supplementary material I might make available in the future.

Registering gives you access to it all.

Visit https://go.askleo.com/regisfree *right now* and register.

That link is mentioned *only here,* and it's totally FREE to owners of this book.

About the Author

I've been writing software in various forms since 1976. In over 18 years at Microsoft, I held both managerial and programming roles in a number of groups, ranging from programming languages to Windows Help, Microsoft Money, and Expedia. Since 2003, I've been answering tech questions at the extremely popular *Ask Leo!* website (https://askleo.com) and in other entrepreneurial projects like this book.

Curious for more? Someone asked, and I answered on the site: Who is Leo? (https://askleo.com/who-is-leo/)

Feedback, Questions, and Contacting Leo

I'd love to hear from you.

Honest.

I truly appreciate reader input, comments, feedback, corrections, and opinions—even when the opinions differ from my own!

Here's how best to contact me:

- If you have a comment or a question about this book, I strongly encourage you to register your book, as outlined in above, and use the prioritized comment form in the registered owner's center.
- If you prefer not to register your book, you can email me at leo@askleo.com.
- If you have a computer or tech-related question, the best approach by far is to first search *Ask Leo!* (https://askleo.com). Many, many questions are already answered right there, and finding those answers is much faster than waiting for me.
- If you can't find your answer using Search, visit https://askleo.com/book and submit your question. That's a special form just for book purchasers and it gets prioritized attention.
- If you just want to drop me a line, or have something you want to share that isn't covered above, you can use https://askleo.com/book, or email leo@askleo.com.
- If you're just not sure what to do … email leo@askleo.com. ☺

Copyright and Administrivia

Please note that much of this publication is based on my own personal experience and anecdotal evidence. Although I've made every reasonable attempt to achieve complete accuracy of the content in this book, I assume no responsibility for errors or omissions. You should use this information as you see fit and at your own risk.

Any trademarks, service marks, product names, or named features are assumed to be the property of their respective owners. They are used only for reference. Unless specifically stated otherwise, use of such terms implies no endorsement.

Sharing this Document

The bottom line is that you shouldn't. More specifically, you shouldn't make copies and give them to others.

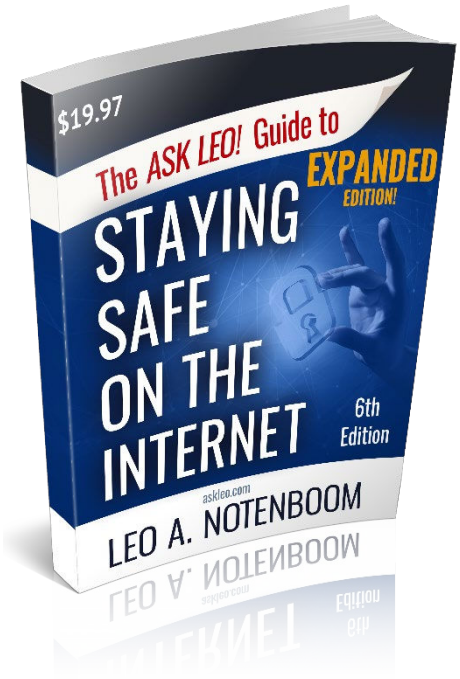
Loan your copy as you see fit. (Back it up, of course!) However, making an additional copy to *give* to someone else is a no-no. (The rule is pretty simple: if you *loan* the book, they have access to it, and you shouldn't, until they return it. If both you and your friend can use the book at the same time, then you've made a *copy,* and that's the part that's wrong.) That also applies to uploading a copy to an electronic bulletin board, website, file sharing, or similar type of service.

The information in this document is copyrighted. That means giving copies to others is actually *illegal*. But more important than that, it's simply wrong.

Instead, if you think it's valuable enough to share, encourage your friends who need this book to buy a copy of their own. Or, heck, buy one as a gift for them.

Remember, it's the sale of valuable information in books like this one that makes Ask Leo! possible. It's pretty simple, really; if enough people disregard that, there'd be no more books, and eventually no more Ask Leo!

The Ask Leo Guide to Staying Safe on the Internet: Expanded Edition



If you've found this FREE ebook valuable, I'd like to introduce you to the EXPANDED edition!

Over twice as big, *The Ask Leo Guide to Staying Safe on the Internet* ***Expanded Edition*** dives deeper into all of the topics we've covered here, as well a few we haven't, to help you to be *even safer* and better prepared.

Click here for more information about the Expanded Edition, including a free sample of the first 10% of the book, including its full table of contents so you can see exactly what's in store.

Before you check out: be sure to use the coupon code EXPANDED to get an additional 25% off the purchase price of *The Ask Leo Guide to Staying Safe on the Internet* ***Expanded Edition***.

More Ask Leo! Books

If you found this book helpful, check out my library of books at https://askleo.com/shop.