

**The ASK LEO! Guide to**

**FREE  
EDITION!**

# STAYING SAFE ON THE INTERNET

4th  
Edition

[askleo.com](http://askleo.com)

**LEO A. NOTENBOOM**

<https://askleo.com>

The Ask Leo! Guide to  
Staying Safe on the Internet

<https://askleo.com>

The Ask Leo! Guide to  
Staying Safe on the Internet

# The Ask Leo Guide to Staying Safe on the Internet

FREE Edition

4th Edition

by

Leo A. Notenboom

<http://askleo.com>

4.01

ISBN: 978-1-937018-41-2

Copyright © 2016 Puget Sound Software, LLC & Leo A. Notenboom  
All rights reserved.

## Table of Contents

The <i>Ask Leo!</i> Manifesto .....	1
First: Another Freebie for You .....	2
Part 1: Protect Yourself.....	3
It Pays to Be Skeptical.....	3
Just What Is Common Sense? .....	7
Stop Spreading Manure .....	14
Part 2. Protect Your Data .....	20
How Do I Back Up My Computer? .....	20
Part 3: Protect Your Computer .....	27
Do I Need a Firewall, and If So, What Kind? .....	27
What Security Software Do You Recommend? .....	31
How Do I Remove Malware? .....	36
How Do I Remove PUPs, Foistware, Drive-bys, Toolbars, and Other Annoying Things I Never Wanted? .....	41
How Do I Make Sure Windows is Up-To-Date?.....	49
Part 4: Protect Your Laptop .....	55
How Do I Use an Open Wi-Fi Hotspot Safely? .....	55
Part 5: Protect Your Online World.....	61
Is the Cloud Dangerous?.....	61
How Long Should a Password Be? .....	66
Why is It So Important to Use a Different Password on Every Site? .....	71
Email Hacked? Seven Things You Need to Do Now .....	76
Afterword.....	83
Register Your Book! .....	84
About the Author.....	85
Feedback, Questions, and Contacting Leo.....	86
Copyright and Administrivia.....	87
Sharing this Document.....	88
The Ask Leo Guide to Staying Safe on the Internet EXPANDED Edition .....	89
More <i>Ask Leo!</i> Books.....	90

## 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 make technology work for you.

I want to replace that *frustration* and *intimidation*  
with the *amazement* and *wonder* 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: Another Freebie for You

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

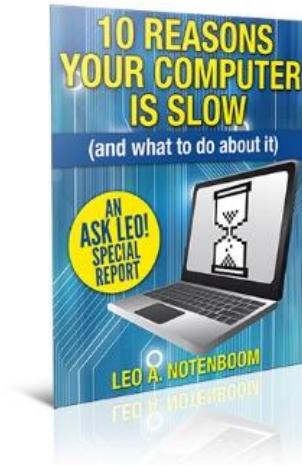
But before we dive in, I have something more for you: my *Ask Leo!* special report, "**10 Reasons Your Computer is Slow (and what to do about it)**". This report will help you identify why your computer is slowing down, and the steps you can take to fix it.

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 web page 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, depending on the circumstances.

#### *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. People generally prefer to trust the people they encounter every day.

Hackers, malware authors, over-aggressive salespeople—essentially just about anyone who wants something—know that. They're often skilled at using your trust against your best interests.

Consider that warning message that popped up...

#### *Warning: malware detected, click to remove ...*



A pop-up message telling you there's malware on your machine 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, it's no surprise that belief might be your first response when such a message appears.

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

Except ... it might not have.

Not yet, anyway.

That message might be completely fake. It could be counting on you to trust that it's legitimate, and click on it to take further action. And that "further action" could actually *install* malware (or worse).

Or, it could be legitimate.

What do you do?

### ***Unable to deliver package, details attached...***

You've probably received email—important-looking email—announcing there's a package on its way to you, and the details are in an attached file.

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.

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.<sup>1</sup>

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 web site, 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.

And yet, each one of those scenarios could, in some cases, also be legitimate.

What do you do?

### ***I'm from Microsoft, and we've detected....***

You're working on your computer one afternoon, and you get a phone call from someone who says they work for Microsoft. They've detected that your computer is causing many

---

<sup>1</sup> I've actually received this scenario *legitimately*, which really surprised me. Of course, most are scams of some sort.



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, if you'll just go to a site and type in a few numbers that 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

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 question before you believe, and ask before you trust.

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

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 actually has your best interests in mind. Is the story they're telling accurate? Verifiably accurate? Do you know—beyond a doubt—that they are who they say they are?

If the answer to any of those questions is “no”, or even “I'm not sure”, *stop*. Stop and take whatever 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.”<sup>2</sup>

## ***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](#), 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](#)”), 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.

---

<sup>2</sup> [Nullius in verba](#), besides being the motto of [The President, Council, and Fellows of the Royal Society of London for Improving Natural Knowledge](#), is also a very fancy way of saying “question everything”. ☺

## 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 this:

*Use common sense.*

One of the most common responses is this:

“Great. Just what, exactly, is that?”

When it comes to technology and safety, “common sense” is incredibly important, and yet downright ill-defined.

Let’s see if we can define it a little. I think many of the “rules” will sound familiar to you.

### ***If it sounds too good to be true...***

As we see so often, many malicious incursions mask themselves as 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.

One key 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*. (Though naturally they also appear when you are looking for something related.)

Look at any web site and you’ll see advertisements. Many are legit and well positioned, but many others are little more than over-the-top attempts to get you to click or download whatever it is 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***

Often 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, quite simply, have nothing to do with anything they’re actually experiencing.

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

The list goes on.

Now, I get 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 that malware isn’t present? How do you know 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 “don’t do something because you might have a problem; do something because you *know* you have a problem.”

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

It should be common sense that every "free" service still has a cost. It may be the advertising you need to look at, it may be the mailing list you need to sign up for, it may be something else entirely, but there is simply no such thing as "free" on the internet.

The most common place people fall into the "free" trap are advertisements of this variety: "FREE Scan! Scan your computer for malware FOR FREE!"

In reality, the advertisement is 100% completely accurate. The scan is completely free. The not-so-free parts? If you want to do anything about what the scan actually finds, you'll need to pay. It's a common sales tactic.

Less reputable programs actually lie to you. They warn you of malware and other scary things you simply don't have, or simply aren't issues. All, of course, in a way that will make it appear that giving them your money to fix it 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 when I encounter it. It works like this:

- A program fails or something goes wrong.
- The user reacts, gets frustrated, or gets lost.
- 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 exactly (and only) 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 that follows, which removes all outrageousness by putting the statement in clearer context, or by providing additional information.

When it comes to your computer, when something goes wrong, please *take the time to read what's on the screen in front of you*. That really is only good, common sense. 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 get 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.<sup>3</sup>

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.

It's simply 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. The reality is that 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.

In reality, the internet can provide 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 just because something is on the internet has absolutely no bearing on its accuracy. Yet we see people go off and act as if it's completely accurate, believing random and misleading statements from vague sources with a less-than-altruistic agenda.

---

<sup>3</sup> That's one reason I took on [heroicstories.org](http://heroicstories.org).

With information coming at you from so many random directions, from sources both reliable and unreliable, it's critical we not believe everything we read just because it's been formatted prettily<sup>4</sup> 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 sense?

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<sup>5</sup> might be in spreading its message. Are they being truthful?

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.

## ***Do your research!***

*Search for yourself.* Learn the basics of how to not only use a good search engine (Google, Bing, or others), but also how best to interpret the results. Understand the

---

<sup>4</sup> 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 I'd figured out how to use a word processor to make it *look* much better than it actually was.

<sup>5</sup> And don't kid yourself, every source has an agenda.

difference between the advertisements that are presented on the search results page and the actual results.

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 or not 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. Many librarians have become valuable resources when trying to understand how best to determine the validity of information you run across online.

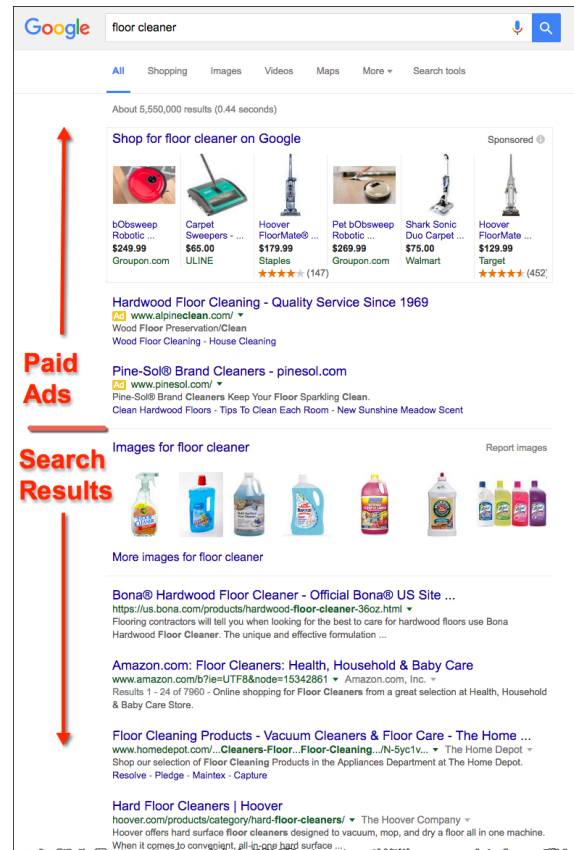
Regardless of who's helping you, it's still okay to be skeptical. When they suggest a site as a trustworthy resource, don't be afraid to ask them why they trust it.

*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 that when enough sites and so-called sources all repeat what only one of them has said, it may feel like it's many sources all coming to the same conclusion. In reality, it's nothing more than a single opinion repeated over and over, known as the "[echo chamber](#)".

Remember that repetition isn't confirmation. You want to find multiple sources that confirm or deny the issue, and do so having arrived at their conclusions independently, using their own research and work.





*Use debunking sites.* I'm a huge believer in using sites like snopes.com, 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.* For just about any topic there are resource sites. Develop a set of sites that you trust. For example, when it comes to technology, I would hope you trust *Ask Leo!* Visit the sites you already trust to 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.

## Stop Spreading Manure

It's an example of yet another brouhaha: a report a few years ago that 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.

That's where things get complicated.

### *Everyone has an agenda*

In the popular television series [House](#), Dr. Gregory House is often quoted as saying, "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.<sup>6</sup>



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

Everyone is a salesman with an agenda. In other words, the information you present is almost always colored by your agenda. People highlight facts that support a particular

---

<sup>6</sup> 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.

agenda, conveniently minimizing or completely ignoring facts that don't. In the worst case, people fabricate "facts" to support their agenda.

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

To be honest, we all do it. Not lie, that is (I would hope); but we color what we say and do with the data that supports our beliefs and opinions, often to the exclusion of objective evidence that might point out the unthinkable:

... we might be wrong.

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

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

As we've noted, most people realize that "If it's on the internet, it must be true" is a sarcastic falsism to express 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. The same people who smile knowingly at that falsism and claim to agree with it will often run out and believe the strangest, most bizarre, completely false things, as long as the information is presented in a way that makes them seem credible.

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

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

### ***We believe what we want to believe***

There are a couple of terms that help explain, at least in part, why that might be.

*Confirmation bias* is the natural tendency we all have to believe what confirms 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](#)).

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 or not we are right.



The *echo chamber* is a term we've been hearing more and more in recent years. It's 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.

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, talk, 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 simply 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](#)
- Drew a sensational [black or white conclusion](#)
- Based on a quote taken [without complete and proper context](#)
- Which was then bounced around the echo chamber on sites [here](#), [here](#), [here](#)<sup>7</sup> and dozens of other media sites.

“  
*One source repeated a thousand times in a thousand places doesn't make it a thousand sources.*

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

Email privacy, and privacy on the internet in general, is a critically important concept. Services like Gmail do process your email to do things like serve related ads that pay for the free service, 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.

However, unless you encrypt your email, it is by definition fundamentally not secure. This is nothing new.

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 understand the agendas those sources might have that color what they present and how they present it.

---

<sup>7</sup> Selected at random from a (irony alert) Google News search on "Google Privacy".

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.](#)



If it 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 actually 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 and important news and information to get the attention it truly deserves.

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

The non-profit world has a term: "donor fatigue". This applies to potential contributors who, while supporting a particular cause or organization, become tired of getting asked for money, time, or whatever repeatedly.

The same is true here.

Call it "manure fatigue". It would be tempting to completely disregard anything found on the internet as likely being bogus.

Unfortunately, there are legitimate outrages, atrocities, and issues of [privacy](#) 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.

## Part 2. Protect Your Data

### 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. Nothing more, nothing less.

The key word in that statement is "copy", as in duplicating the information. After you back up, you have that 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 information from the backed-up copies.

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 away 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, you could lose your data *and* your backup if that hard disk dies.
- If the backup is on a different hard disk, but inside the same computer, you could lose your data and your backup if something happens to the computer that causes both hard disks to be harmed, like a power supply failure.
- If the backup is on an external hard disk, but connected to the same computer, you could lose your data and your backup if there's a software glitch or malware on that computer that starts destroying files on all connected devices.
- 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, but kept in the same *physical* location, you could lose your data *and your backup* if that location suffers a physical catastrophe, such as a fire or flood.

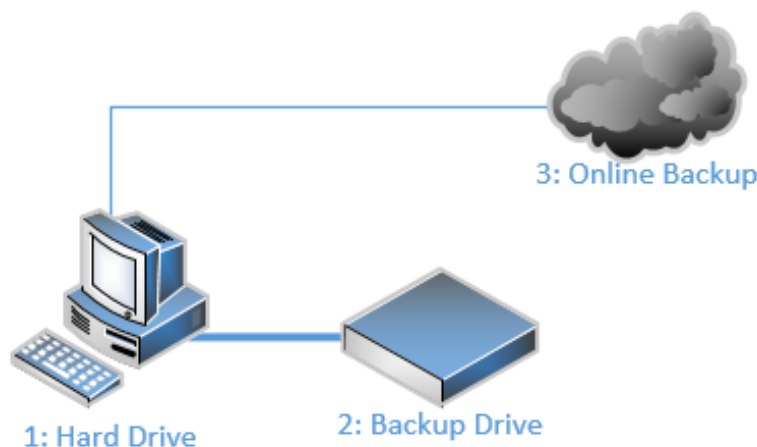
The closer your backup is to the original, the greater the possibility you could lose both at once.

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](#)), 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.

## 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 *physically* means that no matter what happens to your computer or the backups you're creating on-site, 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 you?
- 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 those three scenarios is a great place to start.

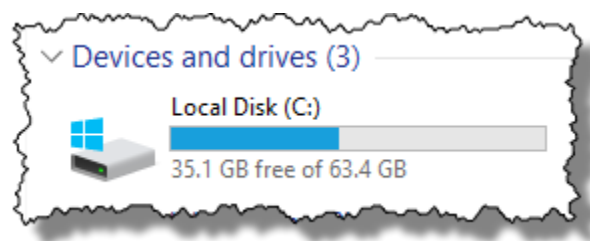
## ***A 1, 2, 3 suggested backup plan***

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.

### **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 not really such a thing as a drive that's "too big".

## 2. Get backup software

I strongly recommend using a dedicated, automated backup program like [Macrium Reflect](#), [EaseUS Todo](#), or an equivalent, and using that tool 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.

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

If you're using Macrium Reflect, I suggest [Saved! Backing Up with Macrium Reflect](#), my ebook that details how to back up your machine using Macrium Reflect. (Multiple digital formats are included, and there's an optional video course as well.)

If you're using EaseUS Todo, then I'll suggest [\*Saved! Backing Up with EaseUS Todo\*](#), my ebook that details how to back up your machine using EaseUS Todo. (Multiple digital formats are included, and there's an optional video course as well.) You might also be interested in a [free series of videos](#) demonstrating how to use EaseUS Todo to create and restore image backups; you can find that [here](#).

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.

## Part 3: Protect Your Computer

### Do I Need a Firewall, and If So, What Kind?

*“ I keep hearing about "firewalls" for my computer and that there are different types. Do I need one? If I do, what kind of firewall do I need?*

The very short, very easy answer is: hell yes! Absolutely, positively you need a firewall.

With all that happens on the internet these days, it's simply too risky to let your computer sit "naked" on the internet. The real question is, what kind of firewall do you need?

The very good news these days is that it's very likely you're already behind a firewall, and don't need to do a thing.

But you should make sure.

#### *What's a firewall?*

Let's be clear: every computer should have or be behind a [firewall](#). Possibly even both.

Firewalls are your first line of defense against an entire class of network-based threat that is constantly (yes, constantly) attempting to attack your computer. Those threats are stopped cold simply by having a firewall.

And there's a good chance you already have one. Possibly even two.

In your car, a firewall is the "wall" of metal between you and the engine. Its purpose is to prevent engine fires from reaching you.

A firewall for your computer is much the same, except that the engine—the network you're connected to—is *always* on fire. The point of a firewall is to keep you from getting burned.

#### *Network-based threats*

A firewall protects your computer from network-based threats.

Almost all computers on the internet are under constant attack. [Malware](#) on other machines, [hackers](#), [botnets](#), and more are waging a slow but extremely persistent war,

probing the internet to find unprotected [vulnerabilities](#) on other internet-connected computers. If they find such a vulnerability, they infect the machine they've found, or worse.

The basic concept of a firewall is very simple: it blocks or filters certain types of network traffic from ever reaching your computer.

Traffic that you want to reach your computer:

- Websites pages you visit
- Software you download
- Music or videos you might watch
- And more...

Other traffic that you definitely don't want:

- Your neighbor's machine, infected with a botnet, trying to connect to your machine over the network to spread the infection.
- Overseas hackers trying to gain entry to your machine over the network to steal your personal information.
- And more ...

A firewall knows the difference.

If you look at the sets of examples above, they differ in one important aspect:

- Things you want are connections that you or your computer initiate. On your order, your computer reaches out and asks for the webpages you visit, the software you download, or the music you listen to.
- Things that you don't want are connections trying to come in from outside.

That's an easy distinction for a firewall to make.

## ***Two basic types of firewalls***

### **Hardware firewalls**

A [router](#) sitting between your computer and the internet is one of the best and most cost-effective firewalls that the typical computer user can have. It's usually a piece of





equipment that sits physically between your computer and where the wires plug into the wall, with flashing lights that tell you it's on duty.

The router's job is to "route" data between the computer(s) and the internet.

Routers also allow you to share an internet connection by what's called "[Network Address Translation](#)". NAT "translates" between the [single IP address](#) you've been given by your internet service provider and the IP addresses assigned to your machines by the router.

Routers watch for connections initiated by your computer reaching out to resources on the internet. When a connection is made, the router keeps track, so when a response comes back on that connection, it knows which of your local machines gets the data.

The side effect is that if an outside computer tries to start a connection, the router doesn't know which computer to send it to. All it can do is ignore the attempt. That effectively blocks everything on the internet from trying to start a connection to a machine on your local network.

And that automatically makes your router a powerful incoming firewall.

Your router will not, however, filter outgoing traffic.

## Software firewalls

Software firewalls are programs that run on your computer. They operate as closely to the network interface as possible, and monitor all your network traffic.

If you're not using a router, all of the network traffic will still technically reach your machine, but the firewall prevents malicious traffic from getting any further. Much like a router, a software firewall prevents the rest of your system from even realizing that there is any malicious traffic.

In addition, some software firewalls can be configured to monitor outgoing traffic. If your machine becomes infected and some malware attempts to "phone home" by connecting to a known malicious site, or tries to infect other machines on your network, a software firewall can warn you and block the attempt.

All current versions of Windows have a software firewall built in and turned on by default. Windows may even annoy you into ensuring that the firewall is either turned on (in Control Panel) or that you're aware of the risks of not having it turned on.

The Windows firewall is primarily an incoming-only firewall.

## ***Choosing and setting up a firewall***

In general, I recommend using a broadband router as your firewall. Since it's very likely you already have one, that means you're pretty much done. (Though you'll want to make sure [it's secure](#).)

There is disagreement. Some believe that [an outgoing firewall is important](#). My position is that an outgoing firewall doesn't really protect—it simply notifies after something bad has happened.

Routers are pretty common, and nearly a requirement for anyone who has more than one computer sharing an internet connection (though I'd recommend you use one even if you have only one computer). If you have a NAT router, you have a firewall without needing to burden each computer with additional software.

Software firewalls do make sense in a very important situation: they are critical when you can't trust other computers on your local network.

[Don't trust the kids'](#) ability to keep their computer safe on the internet? Enable the software firewall on your computer.

Heading out to the local open WiFi hotspot? Turn on the software firewall before you connect.

In later versions of Windows, the built-in firewall has matured to the point where it's actually quite reasonable to leave it on all the time, even if you're behind a router. It seems to impact operations very little, and saves you from remembering to turn it on when you travel or have that not-so-trustworthy guest on your network.

That's why I said earlier that you might, in fact, have two firewalls already: your router and your Windows firewall. And that's quite OK.

## ***What firewalls can't do***

It's important to remember that a firewall can't protect you from everything.

A firewall protects you from threats that arrive via malicious connection attempts from elsewhere on the internet.

A firewall will *not* protect you from things that you invite onto your machine yourself, such as email, attachments, downloads, and removable hard drives.

Nonetheless, protection from network attacks remains critically important.

## 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.

### ***The short-short version***

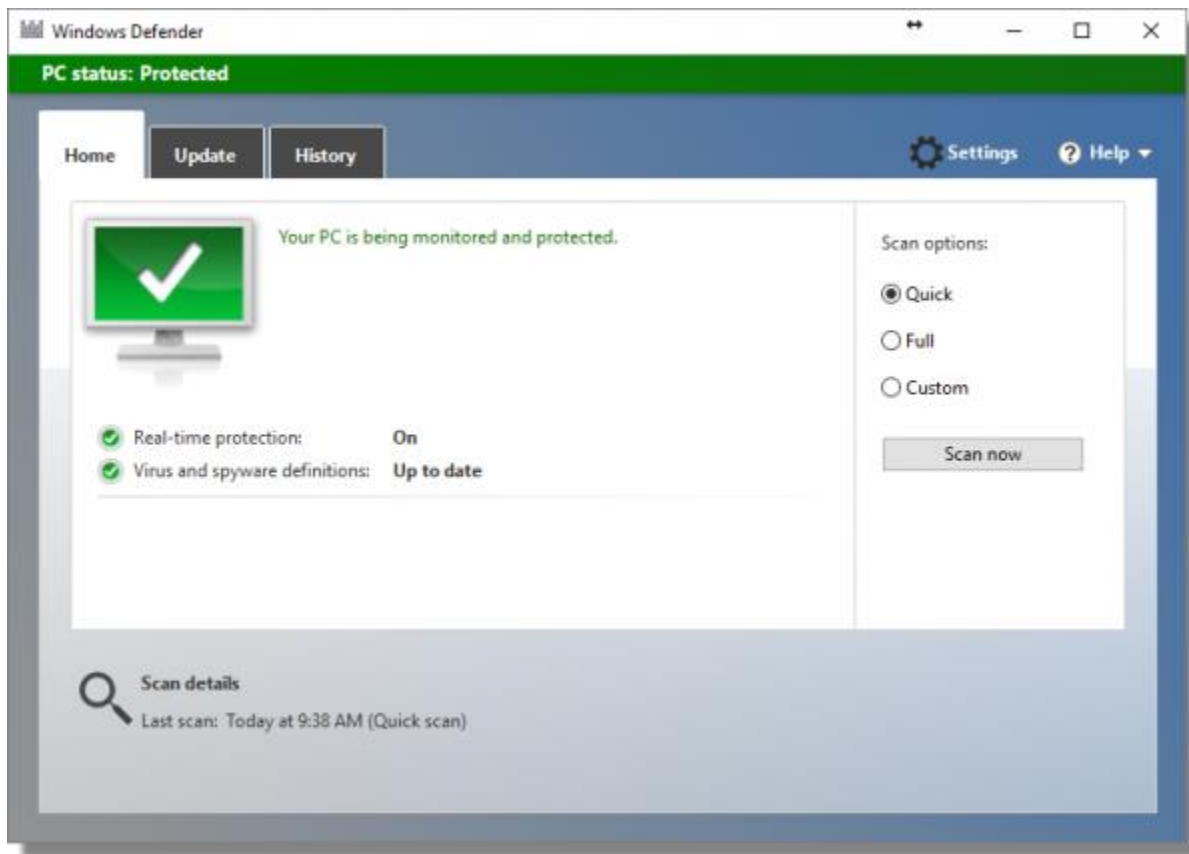
Most home and small-business users who don't want to think about it too much should simply:

- Get a router, even if you have only one computer. This will be your primary firewall.
- Use Windows Defender, already installed in Windows 8, 8.1 and 10, or install the free [Microsoft Security Essentials](#) for earlier versions of Windows. This will be your anti-virus, anti-spyware, and malware scanner.
- Turn on Windows Update to keep your computer as up-to-date as possible.
- Turn on Windows Firewall when you travel; perhaps just leave it on all the time.

That's it.

Good basic protection in four steps with only one download.

## ***Basic security software: Windows Defender***



Windows Defender comes pre-installed in recent versions of Windows. It does a fine job of detecting malware without adversely impacting system performance, and does so without 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.

### **Windows 7 or earlier?**

If you're running a version of Windows prior to Windows 8, you'll want to download and install [Microsoft Security Essentials](#) (MSE). It's the same as Windows Defender, except it's not pre-installed.

**Important:** the "Windows Defender" you might find pre-installed in some earlier versions of Windows is *not* the same—it's only an anti-spyware tool. Current versions of Windows Defender and Microsoft Security Essentials are full anti-malware tools.

## ***The ratings game***

Every so often, Windows Defender comes under fire for rating lower than other security packages in tests published online. As a result, every so often I get push-back—often angry push-back—that Windows Defender 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 very practical reasons I continue to prefer Windows Defender.

- It's free.
- It's already installed in Windows 8 and later; there's nothing you have to do.
- In practice, it rarely impacts system performance.
- It integrates with Windows Update to keep itself up-to-date.
- It has no additional agenda: it's not going to pester you with renewals, upgrades to more powerful versions, or up-sells to tools you don't need.

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

Thus, my recommendation stands. Windows Defender remains a solid, free anti-virus and anti-spyware package with minimal system impact, and should be appropriate for almost anyone.

## ***Alternatives and additions***

On the other hand, I fully recognize that Windows Defender 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 truly free only to discover, instead, a free trial, or a free download (if you want to keep it past a certain length of time, you're required to hand over money).



Some programs have become as much self-promotion tools as they are anti-malware 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** has evolved over the years from a tool that defied categorization (not really anti-virus, not really anti-spyware, but still catching things that other tools did not) to a full-featured anti-malware package. What's important is that it continues to have a very good track record of removing troublesome malware that other packages sometimes miss.

**Spybot Search and Destroy** is one of the longest running and highly regarded anti-spyware tools out there. Like Malwarebytes, it has also expanded to be a more fully-featured anti-malware tool. I used it for many years myself back in its anti-spyware days.

**AVG**, **Avira**, and **Avast**, or the "three AV's", as I like to call them, are three other free solutions I've recommended over the years.

## Caveats with all

I need to reiterate some important points.

1. I'm referring to the free *version* of each of these tools, *not the "Free Trial"*. In several cases they are completely different downloads. A "free trial" is just that—a trial, typically of a more fully-featured product. Unless you know otherwise, the truly FREE version of these tools would be my recommendation.
2. Regardless of which you download, you are still likely to be faced with upgrade and up-sell offers to a more fully featured version, or even an ongoing subscription. Unless or until you *know* you want this, always decline.
3. Speaking of declining: when installing any of these products, always choose custom installation, never the default. You may well get toolbars and other

unrelated software you simply don't need or want. Consider using [Ninite](#) to install these tools—all are available there.

## ***Offline scanner***

If your machine becomes infected with malware of some sort, there's a good chance you won't be able to actually download anything, because the malware will prevent it. That means you won't be able to download the latest update of your anti-malware tools, or perhaps be able to run them at all. When that happens, you need an offline malware scanner.

An offline scanner is simply a complete anti-virus and anti-spyware scanning tool that you download and burn to CD or DVD, or place on a USB memory stick, using another computer. You then boot the infected machine from the media you created, and run the scanner. The infected Windows doesn't run at all, and the scanner can check, change, or repair more than a normal scanner could.

I recommend [Windows Defender Offline](#) for this purpose. Unfortunately, it's not something you download and keep ready to use. In order to make sure you're running the most recent update of the tool and its database of malware, it's important to download it *when you need it* (thus the use of another computer).

## ***What else?***

### **Firewall**

For home and business use, I recommend the use of any good NAT router as a firewall. 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.

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 likely already on by default. There's often 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.

## How Do I Remove Malware?

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, or some other form of malware, and that machine's owner is having a tough time getting rid of it.

And it often happens with anti-malware software installed that "should" have taken care of it before it got to this stage.

Hopefully, that'll never be you. If it is, 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 only one thing I would have you take away from this article, it would be this:

Prevention is much less painful than the cure.

As we'll see in a moment, the steps to remove malware can be painful and time consuming. While it might seem like work, knowing [how to stay safe on the internet](#) is much, much easier in comparison.

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

### *Back up*

My strong recommendation is that you 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.



## ***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.

And, 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, which 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***

Quite often, anti-malware tools will regularly perform a "quick" or fast scan. That's typically quite 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—typically the C: 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 trying additional reputable tools is a reasonable approach.

I recommend the free version of [Malwarebytes' Anti-Malware](#) 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, I have to stress: *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.

They'll 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 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, I'd 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 only 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.

In fact, it's the only way to know that you've removed a virus. Once infected, none of the steps above, *aside from restoring from a backup taken before the infection*, are guaranteed to remove the 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, any and all viruses and malware. This may be part of the next step, as most Windows set-up programs offer to reformat the target hard drive before installing Windows.
- **Reinstall.** Yes, reinstall everything from scratch. Reinstall the operating system from your original installation media. (Or restore the system to an image backup you took when you got the machine, which preserved the "factory original" state.) Reinstall applications from their original media or saved downloads.
- **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 taking care to only copy the data you need, so as not to copy back the malware.
- **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 just generally [learning how to stay safe](#) is much easier than the recovery process I've just outlined.

And having backups 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.

## How Do I Remove PUPs, Foistware, Drive-bys, Toolbars, and Other Annoying Things I Never Wanted?

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

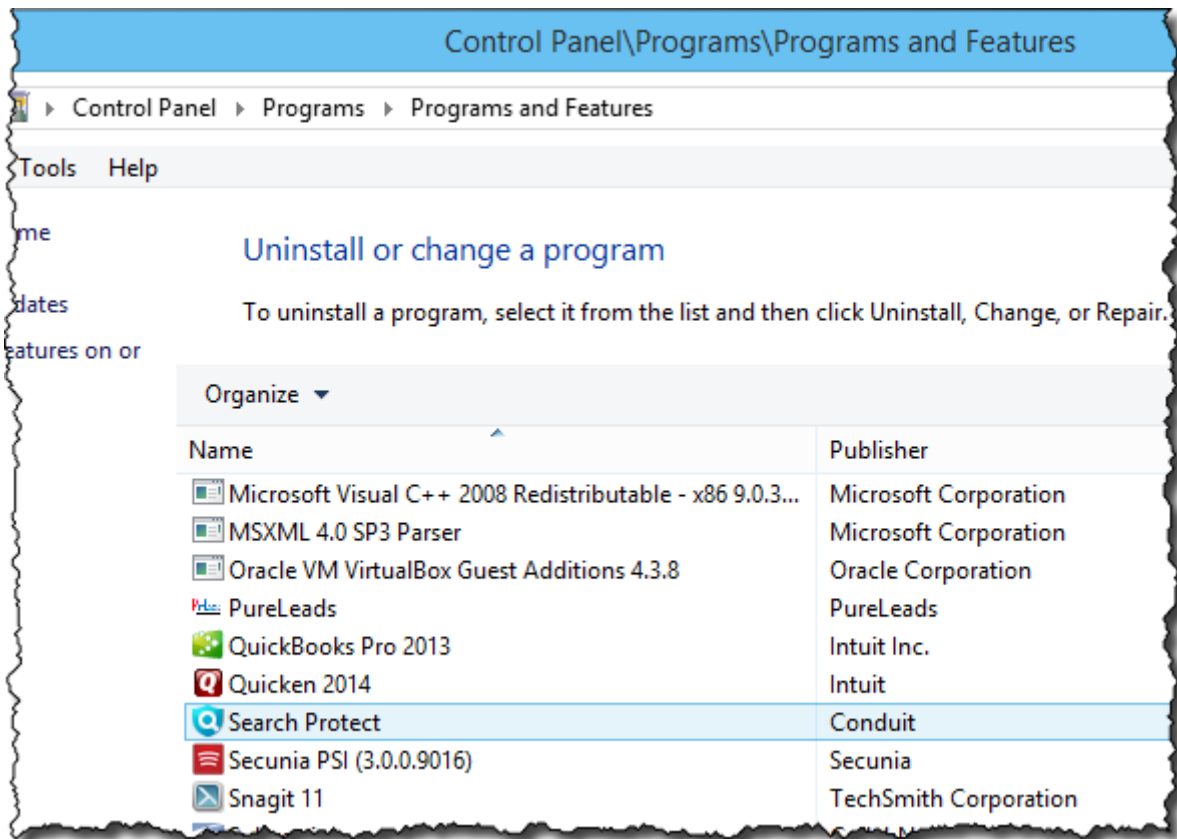
Unfortunately, it's happening more and more. I'd say that PUPs (Potentially Unwanted Programs, although there's rarely any "potentially" about it), rogue toolbars, and search-engine hijacks are some of the most common issues I see in my inbox.

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.

### *Uninstall the somewhat well-behaved PUPs*

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

What that means is that we start in Control Panel's **Programs and Features**.



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.

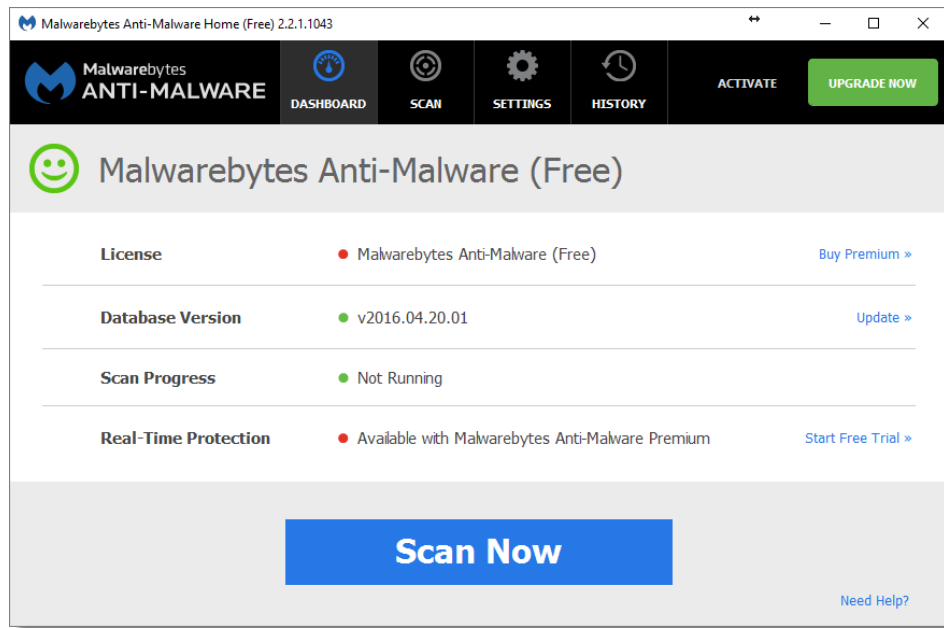
Right-click the item you want to uninstall, and click **Uninstall**.

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 simply cause the PUP to be reinstalled.

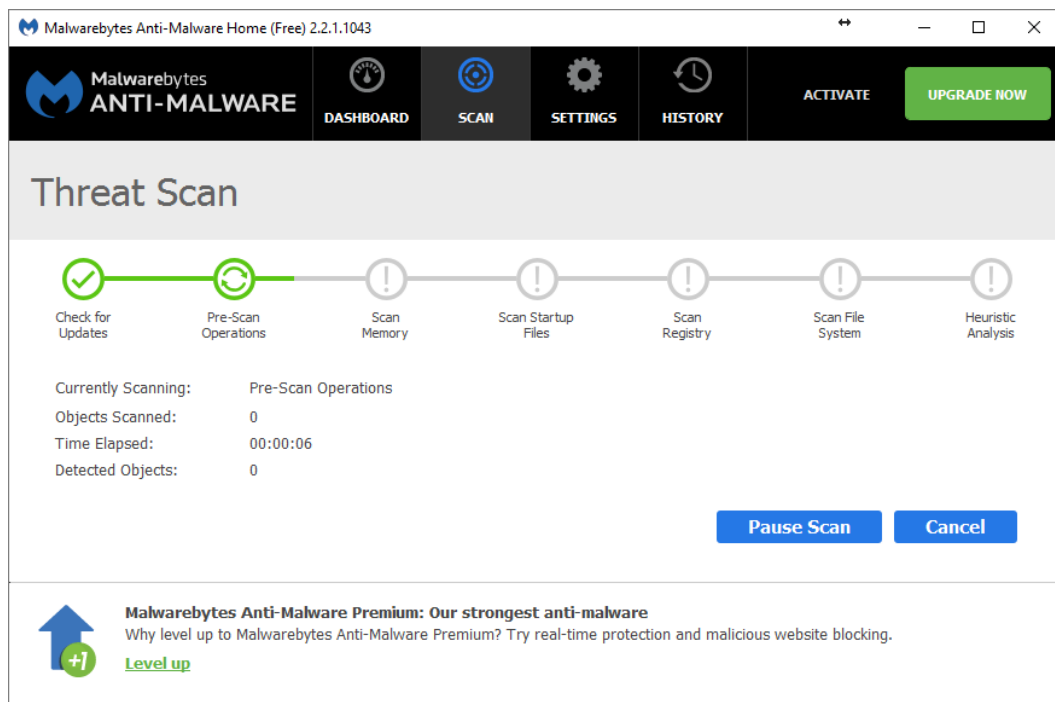
## ***Run MalwareBytes***

If you don't have it already, download and install the [free version of Malwarebytes Anti-Malware](#). (Don't bother selecting the free *trial* of their premium product. While it's good and potentially worth the investment, it's not what you need right now. Stick with the free version.)

After you open the program, it automatically updates its database. Click **Scan Now** to perform a scan.



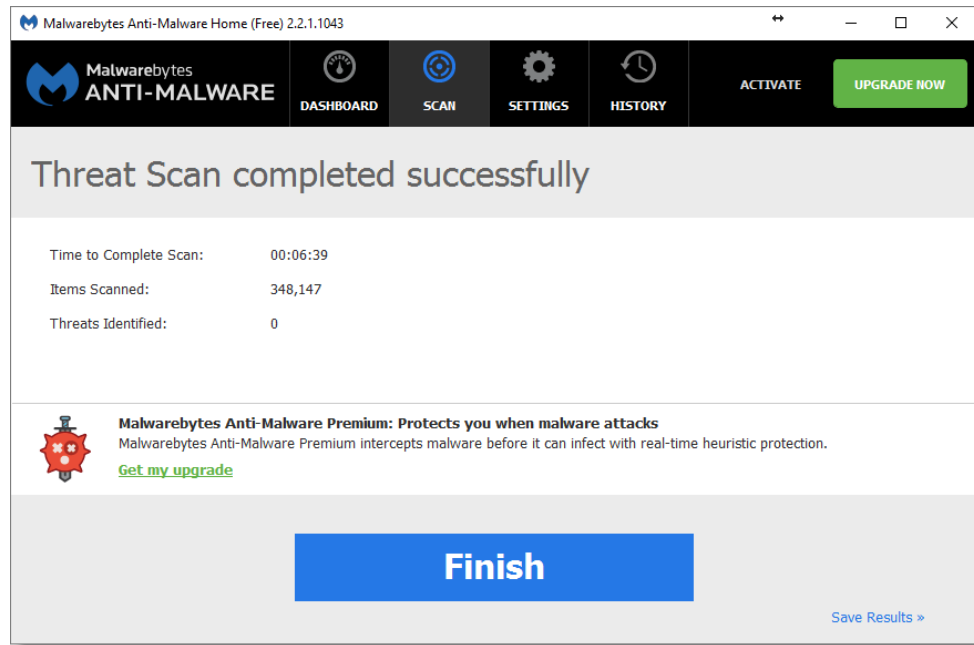
The Malwarebytes scan may take a while.



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.



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***

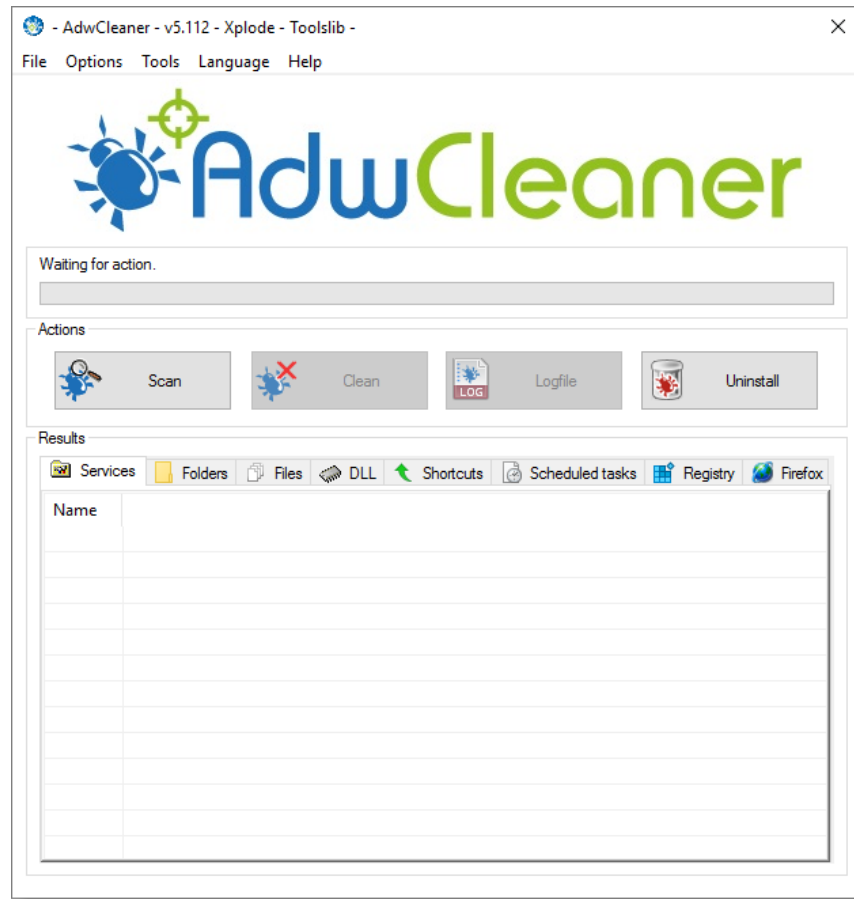
AdwCleaner is perhaps best [downloaded from our friends over at BleepingComputer.com](#). It's actually from France, and if you're not careful, you can easily end up on their French language website (or at least I did). That's not a big deal if you speak French, I suppose, but I don't, and I'm guessing many of you do not as well.

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.



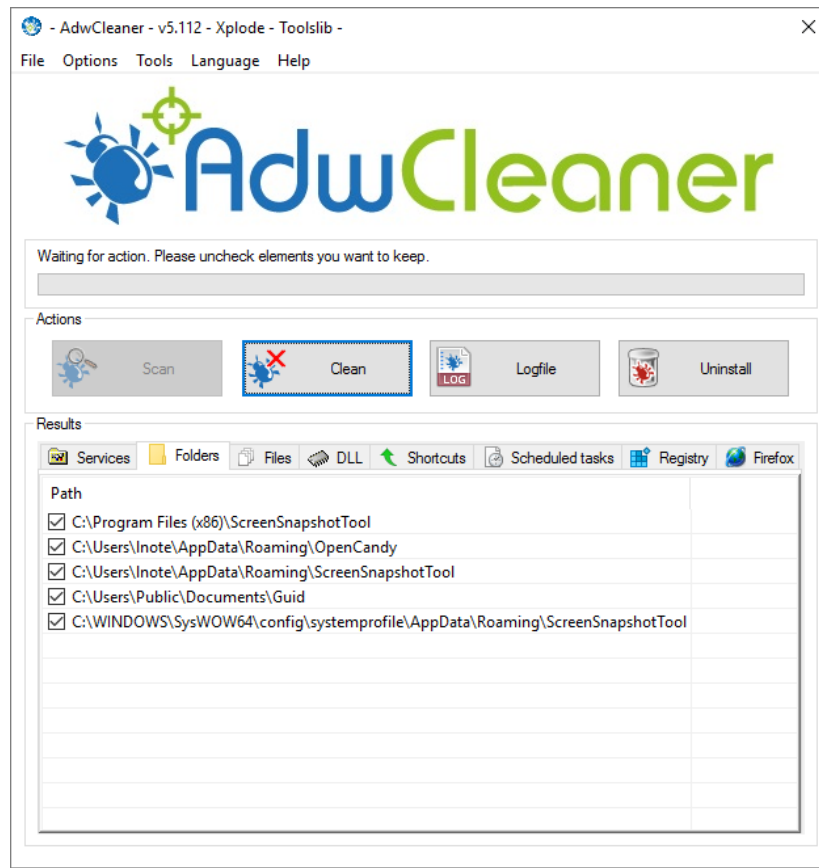
Click **Scan**.



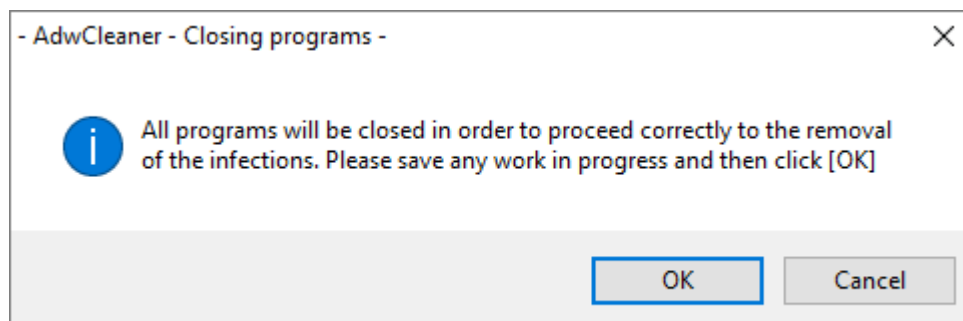
Once the scan is complete, AdwCleaner will present a message: "Waiting for action. Please uncheck elements you want to keep."

Click each of the tabs in the results box at the bottom of the AdwCleaner window. This will list each item it has found which it thinks is a candidate for removal.

Here you can see that AdwCleaner found several folders it thinks should be deleted.

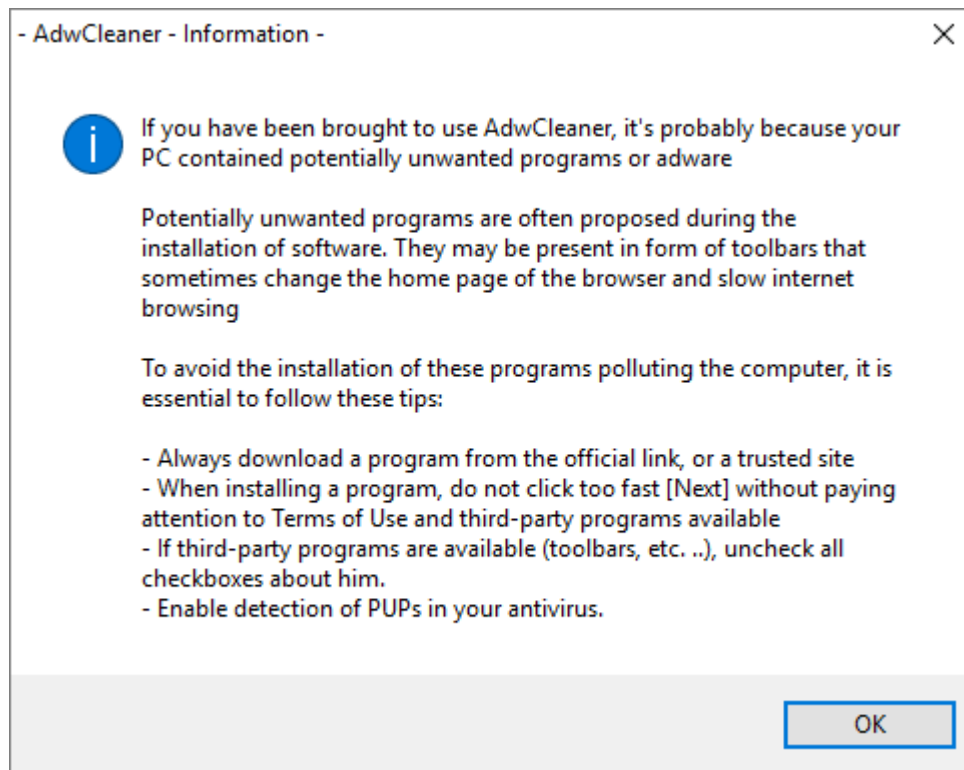


If you're not certain you need it, leave it checked. In other words, go ahead and let AdwCleaner clean up anything you don't recognize by clicking **Clean**. It first warns you that all programs should be closed.

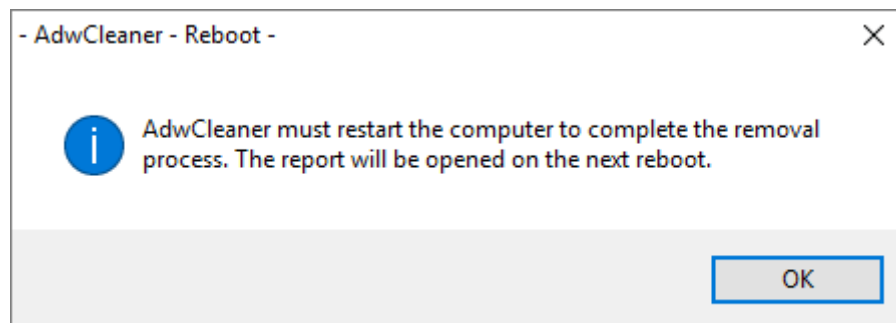


It will close many programs, including some that normally start automatically when you log in. AdwCleaner will likely require a reboot when it's done anyway, so those programs will return then.

AdwCleaner scans, cleans, and presents information on preventing this type of thing from happening in the future, similar to what I'll discuss below.

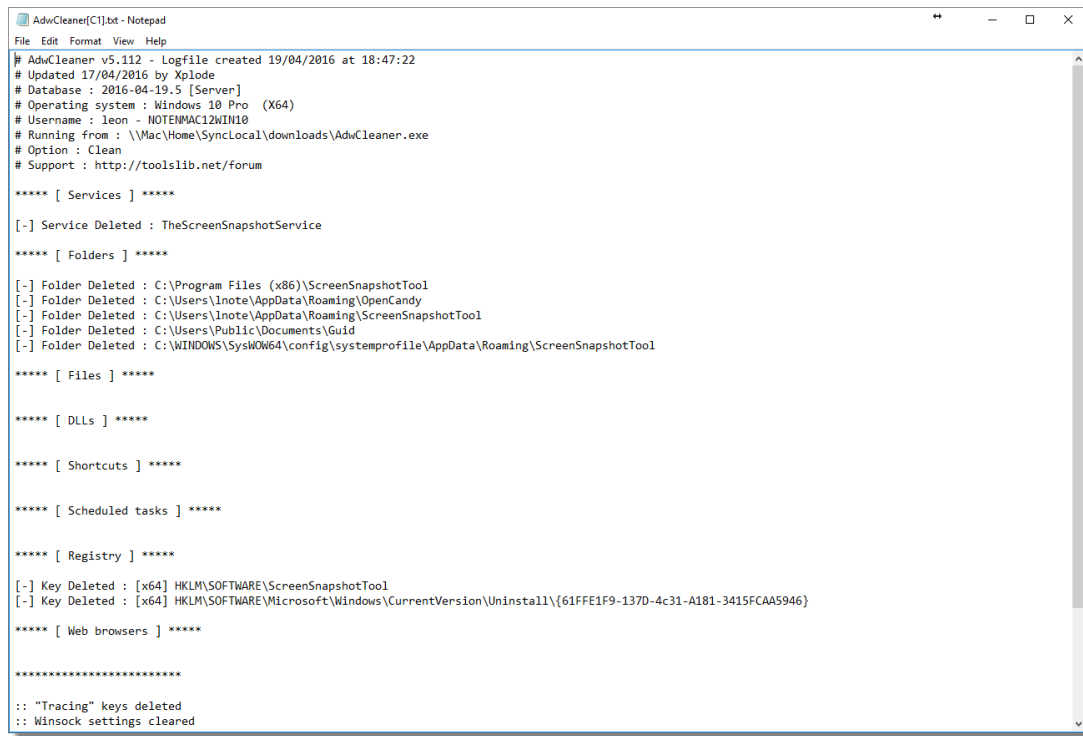


You'll get a Reboot Required message.



Click **OK**, and your machine reboots.

After the reboot, AdwCleaner shows you a text file containing the results log of its operation in Notepad.



```
AdvCleaner v5.112 - Logfile created 19/04/2016 at 18:47:22
# Updated 17/04/2016 by Xplode
# Database : 2016-04-19.5 [Server]
# Operating system : Windows 10 Pro (X64)
# Username : leon - NOTEMAC12WIN10
# Running from : \\Mac\Home\SyncLocal\downloads\AdvCleaner.exe
# Option : Clean
# Support : http://toolslib.net/forum

***** [ Services ] *****

[-] Service Deleted : TheScreenSnapshotService

***** [ Folders ] *****

[-] Folder Deleted : C:\Program Files (x86)\ScreenSnapshotTool
[-] Folder Deleted : C:\Users\leon\AppData\Roaming\OpenCandy
[-] Folder Deleted : C:\Users\leon\AppData\Roaming\ScreenSnapshotTool
[-] Folder Deleted : C:\Users\Public\Documents\Guid
[-] Folder Deleted : C:\WINDOWS\System64\config\systemprofile\AppData\Roaming\ScreenSnapshotTool

***** [ Files ] *****

***** [ DLLs ] *****

***** [ Shortcuts ] *****

***** [ Scheduled tasks ] *****

***** [ Registry ] *****

[-] Key Deleted : [x64] HKLM\SOFTWARE\ScreenSnapshotTool
[-] Key Deleted : [x64] HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{61FFE1F9-137D-4c31-A181-3415FCAA5946}

***** [ Web browsers ] *****

*****

:: "Tracing" keys deleted
:: Winsock settings cleared
```

You can just close Notepad at this point.

## ***The ultimate removal***

Now, 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.

So, it's worthwhile to consider restoring to a [recent backup image](#). 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'll work. 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 the most common method is by being "offered" to you when you install something else. Often, the offer is hidden and

defaulted to Yes. The technicality 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.

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's offering you something that is not clearly related to the software you want, *uncheck it*. If it's offering to change your search page, *uncheck it*. If it's offering to install some toolbar, *uncheck it*.

You get the idea.

The bottom line is that 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" about it.

## 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.

The good news is that in most recent versions of Windows, you need do nothing. Windows will update itself regularly.

The not-so-good-news? In Windows 10, it'll do so whether you want it to, or not.

Let's look at how we got here, what "here" really looks like, what control you do or do not have, and what I believe you should do.

## ***Vulnerabilities and updates***

The issue is common to all software: no one is perfect. All software has [bugs](#), period, no exceptions.<sup>8</sup>

While many bugs are minor and 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 that takes advantage of them is termed "malicious software", or simply "[malware](#)".

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

It's important, then, that the users of affected software actually take the steps to install those updates when they're made available.

Unfortunately, particularly early in Windows history, individuals often did not install updates, for a variety of reasons. This left their computers vulnerable to more and more malware, even though those bugs had been fixed in subsequent updates.

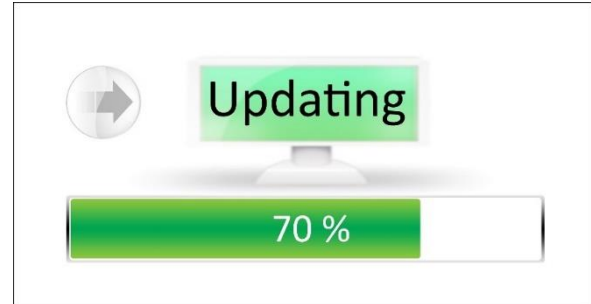
## ***Automating updates***

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

---

<sup>8</sup> If someone claims that a particular bit of software has no bugs, then either they simply haven't yet found the bugs that actually 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's a service that runs in the background, periodically checking for updates to Windows<sup>9</sup> that apply to your machine's particular configuration. When available updates are found, Windows Update can do several different things, depending on how it's configured.



- It can simply notify you that updates are available. You are still responsible for taking the next step: downloading and installing them.
- It can download updates that apply to your computer and notify you they're ready to be installed. You are still responsible for taking the next step: actually installing them.
- It can download the updates that apply to your computer and install them automatically, according to a schedule that you specify.

The reason that schedule is important is that it's not at all uncommon for updates to require your machine be rebooted. Software cannot be updated if it's actually in use. That means in order to update core components of Windows itself, Windows needs to shut down briefly for the update to be possible. That's a reboot.

## *Updates and failures*

Earlier, I said: "The issue is common to all software: no one is perfect. All software has bugs, period, no exceptions."

Updates themselves are software, and in turn can have bugs. The update process itself could have bugs.

The net result is that for a time, Windows Updates themselves were considered "risky". There was a perception that with any given update, your machine could become less stable. In the worst cases, there were Windows updates that actually completely crashed the machine on which they'd been installed. That bad reputation—whether warranted or not—has had some serious and long-term consequences.

---

<sup>9</sup> And optionally, other Microsoft software.

## ***Failures to update***

Because of that bad reputation, some computer users would delay their updates to what they considered to be a safe time—after some period of time had passed that allowed them to feel confident that the update would not harm their machine.

Others stopped taking updates altogether.

Needless to say, the authors of malware approve. To them, delaying or skipping updates means that 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 that fixes it.

Applying updates regularly remains the best approach to keeping your system secure and up-to-date. I continue to recommend that you let Windows update itself automatically, so you don't have to take any action at all. As we'll see in a moment, Microsoft agrees—strongly.

Perhaps a bit too strongly.

## ***Windows 10 and forced automated updates***

When Windows 10 was released, the options to delay updates were removed from the consumer editions of the operating system. Updates are downloaded automatically and installed automatically.

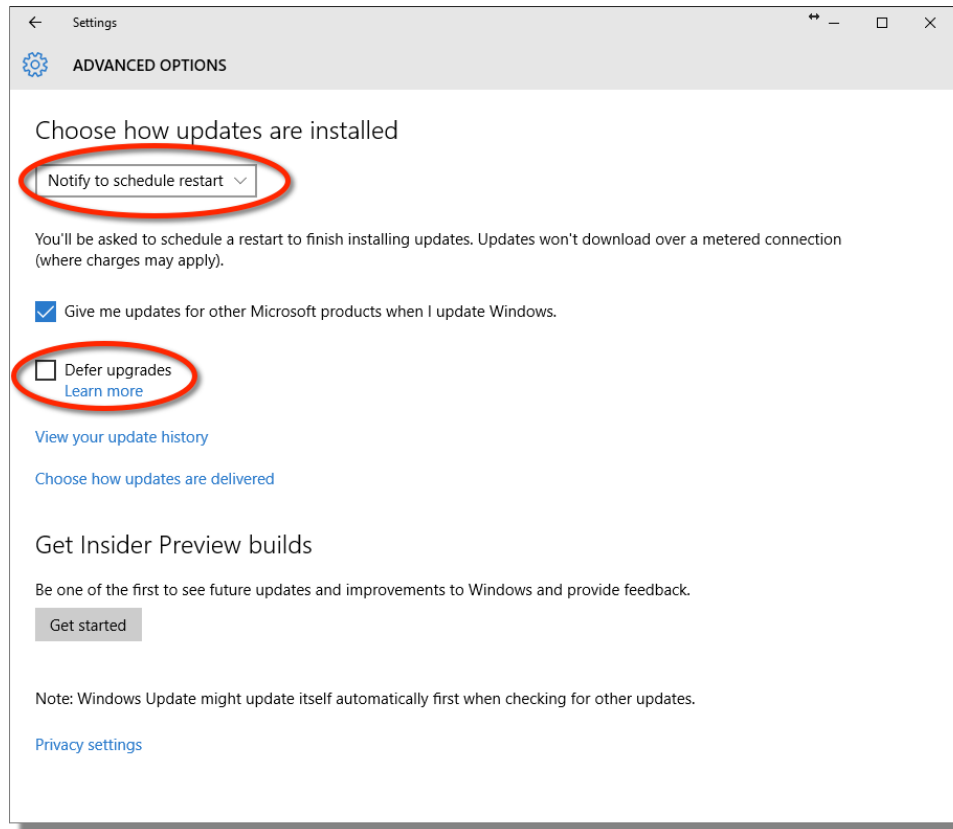
In a perfect world, this would be a perfect solution.

Unfortunately, all software has bugs, and as a result, there have been two major issues:

- While the stability of Windows updates had been improving over time—fewer and fewer updates actually cause any significant problem—some Windows 10 updates, at least initially, seemed a step backwards. Reports of people having problems after an update seemed to increase.
- Updates that required a reboot would indeed reboot, often at an inconvenient time.

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





In **Settings, Windows Update, Advanced Options**, you'll find the following:

- An option to "Notify to schedule restart". While the alternative "Automatic" remains Microsoft's recommended setting, "Notify..." allows you to control when your machine will reboot, and thus allows you to save your work and make sure that nothing will be negatively impacted by the reboot.
- An option to "Defer upgrades". Note that an *upgrade* is not the same as an *update*. Deferring upgrades will delay the arrival of new features and functionality in Windows, but it will not delay the download and installation of bug fixes and security updates.

But 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***

Honestly, it's all about risk management: trading off the risk of a misbehaving update compared 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 regularly. Ideally, perform system image backups 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.
2. If it's an option, configure Windows to automatically download all updates, both for Windows and other Microsoft products.
3. If it's an option, configure Windows to notify you when updates are ready to install. If it's not an option, at least configure Windows to notify you to schedule any restart required after automatically installing updates.
4. Regardless of what notification you get, act on it as soon as is convenient. Install the updates and reboot as needed.

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 unrelated.

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

It can be absolutely safe to send and receive email from a coffee shop, or any 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.

#### ***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.

When you're on an open Wi-Fi hotspot, or connected directly to the internet via other means, that software firewall isn't redundant. In fact, it's *critical*.

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

#### **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, using WPA2, prevents that.

**An interstitial page is not encryption.** If you connect to a hotspot and *the operating system on your machine* requires a password for that to work, that's not an open Wi-Fi hotspot, and you may be OK. On the other hand, if you can connect, and when you fire up your browser it first takes you to a *web page* that says "enter a password" (as in a hotel) or "check to accept our terms" (as in most other open hotspots) **that is not encrypted**, and it is not secure. It is an *open* Wi-Fi hotspot.

## ***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, such as 26, 465, or 587, instead of the default 25.

The exact settings, and whether or not this is even possible, depends entirely on your email service provider; you'll need to check with them to determine the correct settings. How you configure these settings, of course, depends on the email program you use.

With these 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 and that it *keeps on using* that **httpS** connection throughout your email session.

Fortunately, most of the major email services have moved to making **https** the standard, (and sometimes the only) connection method.

Accessing email using a plain http connection might well be the source of many open Wi-Fi-related hacks. I expect that people simply log in to their web-based email service without thinking about security; as a result, their username and password are visible to any hackers in range who care to look.

Be careful. Some services will use https only for your login, which is insufficient, as your email conversations thereafter could be viewed by others. Other services may "fall out" of https, reverting to unsecure http without warning.

## ***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 should be avoided completely while you're using an open Wi-Fi hotspot.

With more and more services being provided online, this is getting to be a larger problem.



Using "the cloud" is a great way to manage your digital life from wherever you may be, but one of the key problems remains security. Using https is critical to that security 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. 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.

## *Use different passwords*

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

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.

## *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.

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 can 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.** Occasionally referred to as "air cards", these are USB devices that attach to your computer and act as a modem, providing 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](#), including a WPA2 password, so as not to be simply another *open* Wi-Fi hotspot susceptible to hacking.

I travel with a MiFi, and also 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, laptops are also easily stolen.

Unfortunately, it only takes a few seconds for an unattended laptop to disappear. That's one reason 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 is completely trustworthy.

In that same vein, I also prepare somewhat 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, which is not mounted unless I need something.
- LastPass, 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 LastPass.
- I have tracking/remote wiping software installed.

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 worth it as well.

## ***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 also relatively easy to be safe.



## Part 5: Protect Your Online World

### Is the Cloud Dangerous?

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

*"That's why the cloud is dangerous."*

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

I disagree strongly.

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...

... as well as a number of things you're already doing, and have been doing 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 recently was this: "[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 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, and you've been using it already—probably for years—and almost certainly before that silly name was attached to it.

So let's jettison the name and all the baggage comes with it, and call this 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 online services are becoming, on average, *safer* than ever before, as service providers learn from mistakes and implement industry best practices.<sup>10</sup>

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*

---

<sup>10</sup> 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 actually getting better. The state of the art in online security is improving overall. If it seems like it's 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.

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.

## ***But we're at the mercy of service providers***

At this point, many folks will 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.

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 you and I have to deal with is that ultimately, service providers are staffed by humans, and humans make mistakes. Saying mistakes should never happen is unrealistic.

Worse, 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](#) 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 (even 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 that 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, plus maybe one or two new ones.

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

- Back up. If it's only in one place, it's not backed up.
- Use strong passwords, and set up and [keep current all account recovery information](#). Use extra security, such as two-factor authentication, if supported.
- 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](#).
- Don't link your important accounts together in such a way that breaching one opens the door to all of them; use different passwords (and perhaps even different email addresses) for each.
- Keep your software up to date, scan for malware, and all of the other items commonly listed [to keep your computer safe on the internet](#).

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](#), 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 common, popular online services can't be used safely—at least as safely as the services you're already using.

Used properly, they can 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 not only taking reasonable precautions to prevent a problem, but also 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.

“

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.

His story: [Mat Honan: How I Resurrected My Digital Life After an Epic Hacking](#).

## 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.

A password today should have a minimum of 12 characters, and ideally, 16 or even 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 might now have access to your account names and passwords. If the service was storing your *actual* passwords, that could indeed be the case. (As I've said before, if a service is storing your *actual* passwords<sup>11</sup>, they simply don't understand security, or they have made some horrifically bad decisions.)

In fact, most services store 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 "5e884898da28047151doe56f8dc6292773603dod6aabbdd62a11ef721d1542d8", which is the hash value that corresponds to that password.<sup>12</sup>

What that means is that hackers do *not* get a list of user names 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?

---

<sup>11</sup> 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.

<sup>12</sup> For the technically 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.

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; they're slow, and will quickly deny further access after too many attempts. But this technique works wonderfully if the hacker has the entire database of account and password hashes sitting on his computer.

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 in a short amount of time.

That's why you're not using that kind of password, 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.

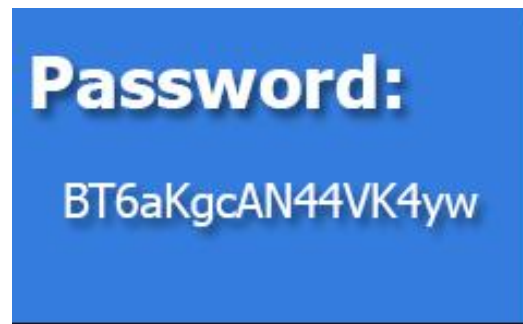
## ***Brute force attacks***

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<sup>13</sup>, or over 221 trillion, combinations.<sup>14</sup>



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 and constructed using upper and lower case letters and numbers, the hackers now have it—even if it was hashed by the service they stole it from.

## ***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). Thee the offline brute-force guessing time in this case would be measured in *centuries*.

Sixteen takes the calculation off the chart. Today.

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

## ***What about special characters?***

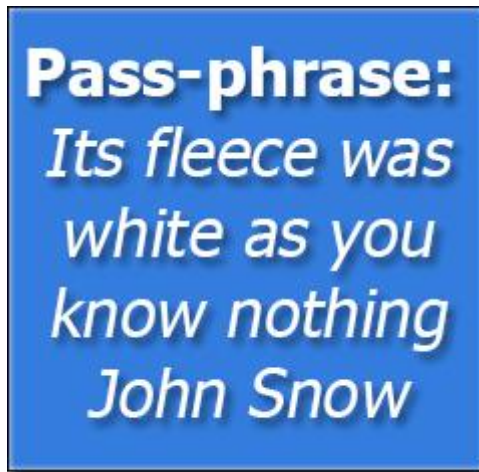
I did leave out special characters, it's true.

---

<sup>13</sup> 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.

<sup>14</sup> 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.





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.

Compare that to sticking with the original 62 letters and numbers, but adding only a single character to make it a nine-character password.

That takes us to over 13 *quadrillion* possibilities.

Yes, adding special characters makes your password better, but significantly better *yet* is to simply 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 *passphrase*? Because they're easier to remember, and they're easier to make long—and as we saw, password length is perhaps the single easiest way to increase the security of a password.

"BT6aKgcAN44VK4yw" is a very nice, 16-character long, secure password that's difficult to remember. In fact, the only way to use this is with a password manager of some sort 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.<sup>15</sup>

---

<sup>15</sup> 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.

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 the brute-force attacks significantly harder ... and yet many use techniques which 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, 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, 16 if at all possible.
- **Use even longer passphrases** where they're supported, or where information is particularly sensitive. I use one for sensitive TrueCrypt volumes, for example.
- **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.

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

## Why is It So Important to Use a Different Password on Every Site?

“

*I keep hearing I'm supposed to use a different password on every internet site where I have an account. What a pain! I can't remember all of those passwords. Yeah, I know. You want me to use a password manager thing, but that seems like putting a bunch of really important things into a single basket. What if that basket gets hacked? I use a strong password, why isn't that enough?*

I'm sorry, but a single strong password just isn't enough anymore. You must use *different* strong passwords on every site where you have an account—at least, every important site.

And yes, you must devise a way to manage them all.

Let me run down an example scenario that's causing all of this emphasis on multiple different passwords.

### ***The all-too-common scenario***

The scenario I'm about to describe is very common. While the specifics won't apply to you exactly, it'll conceptually illustrate what can happen.

Let's say you have an account at some online service—I'll call it Service A. In addition, you have a Yahoo! account because you use Flickr, a Google account because you use Gmail and a number of other Google services, a Microsoft account because you have Windows, and we'll throw in a Dropbox account because you've been listening to me recommend it. You probably have other accounts I haven't listed here, but you get the idea. You have lots of accounts to a number of online services.

You have a wonderfully strong password: 14 completely random characters that you've memorized.

And you use that same wonderfully strong password *everywhere*.

Here's how it can go horribly, horribly wrong.

### ***Anatomy of a hack***

Service A has the best of intentions, but honestly, they don't "get" security. Perhaps they store passwords in their database in plain text, allowing anyone with access to see them. They do that because it's easy, it's fast, and it allows them to solve the problem quickly.

They make the assumption that the database containing your password will be impenetrable.

Hackers *love* it when site designers make assumptions like that because, of course, the assumption is false.

One day, a hacker breaches site security and steals a copy of the customer/user database. The hacker walks away with a database that contains the following information for every user:

- Their log-in ID
- The email address associated with the account
- The password (or enough information from which the password can be determined)<sup>16</sup>
- Password hints



They can log in to your account on Service A. That may or may not be a big deal, depending on exactly what Service A is and how you use it.

But it opens a very dangerous door.

## ***It doesn't have to be a hack***

It's important to understand that while this example centers around what we hear about in the news most often—the hack of an online service and the theft of their user database—it's certainly not limited to that.

Essentially, anything that could compromise your password brings you to this point. That includes:

- Sharing it with the wrong person.
- Keyloggers and other malware sniffing your password as you type it in.

---

<sup>16</sup> Thankfully, services rarely store the actual password—though of course they could. (If your service can tell you your actual password, then they're doing it wrong, and they've stored the password itself somewhere). Rather, they store what's called a "[hash](#)" of the password. Depending on several factors—typically, poor decisions made by whoever implemented the authentication mechanism—it is occasionally possible for hackers to indirectly reverse-engineer passwords from hashes.

- Improper use of an open Wi-Fi hotspot.

And so on.

Anything that puts your single password into the hands of a malicious individual puts you at greater risk than you might assume.

## ***Password skeet shooting***

Once they have your password, the hackers go hunting.

As most people have accounts on one or more of the major services I mentioned, the hackers start trying the information from Service A as if it were the correct information for Gmail, Outlook.com, Yahoo, Facebook, Twitter, Dropbox, and more.

They try your email address and password to log in to the email service you're using.

They try your log-in ID and password (or that email address and password) on as many other services as they can.

And very often, *it works*. The hackers gain access to another account of yours that was completely unrelated to the initial security breach.

Unrelated, of course, except that you used the same password at both.

[If you use the same password everywhere, a single leak of that password puts all your accounts at risk](#). Hackers will be able to log in to your other online accounts as well. Maybe not all; maybe only a few...

...but a few is all it takes.

## ***The weakest link***

Note that this has absolutely nothing to do with the security expertise of the sites where your account is eventually compromised. That Gmail, Outlook.com, Yahoo, and others have excellent security didn't factor into this at all.

Service A was the weakest link. Their security wasn't up to the task. Their database was breached. Their information was leaked. Your account information and password—the password you use everywhere—was exposed.

Service A was at fault.

But the real problem is your use of that single password everywhere.

## ***It shouldn't be this way***

I'll happily admit that things like this shouldn't happen.

But they do. Not terribly often, but often enough.

And most services are better at security than our fictional Service A.

But it's also not a black-or-white equation. Even large corporations that either should know better, or simply miss things, can put your information at risk. For example, a hack at Adobe a couple of years ago had the potential to [expose the passwords of 130 million Adobe account holders](#). It's not as obviously stupid as storing passwords in plain text, but to security experts, it comes surprisingly close.

I hate to say you can't trust anyone, but ultimately ... you *shouldn't* trust anyone not to accidentally expose your password.

And, as I mentioned above, it doesn't have to be a big service breach for there to be a problem.

Using a different password on each site limits your exposure if any of those sites are compromised.

## ***Managing lots of passwords***

So it comes down to how to manage a lot of different (and long and complex) passwords.

I still recommend [LastPass](#) and use it myself.

Doesn't that put all my eggs in one basket?

Yes, it does. But it's a very good basket. And I've taken additional steps to ensure that it stays that way.

I talk about LastPass in more depth in [LastPass—Securely keep track of multiple passwords on multiple devices](#), but I'll highlight two important reasons I consider LastPass secure:

- The people at LastPass don't know your master password. They couldn't tell you what it is if they wanted to. They cannot access your data at all; all they can see is the encrypted data. Even if a hacker were to somehow gain access to their

databases, [\*which has never, ever happened\*](#), the hacker would also be unable to decrypt and view your information, because LastPass does encryption right. Decryption happens locally on your machine, so the only thing ever transmitted between your computer and LastPass is the encrypted data.

- In addition to using a strong password (of course), LastPass supports two-factor authentication, and I've enabled it on my account. If you somehow get my master password, you'd still need my second factor *in your possession* to be able to unlock my LastPass vault.

Ultimately, it's up to you. There are several password managers out there, but LastPass is the one I trust.

## ***The very short bottom line***

My recommendation remains:

- Use long, strong passwords: 12-character minimum, randomly generated (there are several tools available, including one in LastPass). Alternately, and if allowed, use a [\*passphrase\*](#) at least four words long, ideally with spaces.
- Use a different password for every log-in account you have. *Every one.*
- Use a password manager like LastPass to keep track of them all for you.
- Use a strong password or *passphrase* on LastPass itself.
- Consider enabling [\*two-factor authentication\*](#) on LastPass for additional security of that very important basket of information.

## Email Hacked? Seven Things You Need to Do Now

Unfortunately, I get questions about hacked email accounts nearly every day.

Someone somewhere has gained access to your account and is using it to send spam. Sometimes passwords are changed, sometimes not. Sometimes traces are left, sometimes not. Sometimes everything in the account is erased—both contacts and saved email—and sometimes not.

But the one thing all of these events share is that suddenly, people (usually those on your contact list) start getting email from "you" that you didn't send at all.

Your email account has been hacked.

Here's what you need to do next.

### ***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 *know* you're using the right password, 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.

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.

**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 the next two items. 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](#): easy to remember, difficult to guess, and long. In fact, the [longer the better](#), but make sure your new password is at least 10 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 here.

*Changing your password is not enough.*

## ***3. Change 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: when you finally do change your password, the hacker can follow the "I forgot my password" steps and *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. They don't have to match the questions (you might say your mother's maiden name is "Microsoft"); all that matters is that the answers you give during a future account recovery match the answers you set here today.

- **Check the alternate email address(es)** associated with your account and remove any you don't recognize or that are no longer accessible to you. The hacker could have added his own. Make sure all alternate email addresses are accounts that belong to you, and you can access them.
- **Check any phone numbers** associated with the account. The hacker could have set their own. Remove any you don't recognize, and make sure that if a phone number is provided, it's yours and you have access to it.

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.

#### ***4. Check related accounts***

This is perhaps the scariest and most time-consuming aspect of account recovery.

Fortunately, it's not common, but the risks are high, so understanding this is important.

While the hacker has access to your account, they have access to your email, including what is in your account now 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 what 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 ... to which the hacker has access.

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 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 proactively changing the passwords on those accounts as well. (There's a strong argument for checking or changing the recovery information for these accounts, just as you checked for your email account, for all the same reasons.)

## **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 will often set an auto-responder 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 actually sent it.

If your account includes the ability to set a different email address to reply to, make sure that's not been set. Check to make sure your email is not being automatically forwarded to another email address.

Similarly, hackers often set up a signature, so every email you send includes whatever it is they're promoting—often a link to a malicious web site.

Make sure to check any signature or automated response features once you regain access to your account.

## **5. 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.

## **6. 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.

## 7. *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*.
- Don't fall for email phishing attempts. If they [ask for your password, they are bogus](#). Don't share your password with anyone.
- 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](#).
- Keep the operating system and other software on your machine up-to-date, and run [up-to-date anti-malware tools](#).
- Learn to [use the internet safely](#).
- Consider [multi-factor authentication](#) (in which simply knowing the password is not enough to gain access). More and more services are starting to support this, and for those that do (Gmail, for example), it's worth considering.

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.

## 8. *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.

## ***9. Share this article***

As I said, email account theft is rampant.

If one of your friends or acquaintances falls victim, share this short-URL:  
<https://askleo.com/hacked> to go directly to a version of this chapter online.

## ***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](#). So, yes, absolutely, scan it for malware and use it 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.

## **Afterword**

I hope this book helps you protect yourself against all the nasty things that happen to you in our internet-connected world.

If it's helped you at all, I consider this a success.

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 to this free 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/registfree> *right now* and register.

That link is mentioned *only here*, and it's totally FREE.



## 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 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/)  
(<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](mailto: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](mailto:leo@askleo.com).
- If you're just not sure what to do ... email [leo@askleo.com](mailto:leo@askleo.com). ☺

## **Copyright and Administrvia**

This publication is protected under the U.S. Copyright Act of 1974 and all other applicable international, federal, state, and local laws. All rights are reserved.

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.

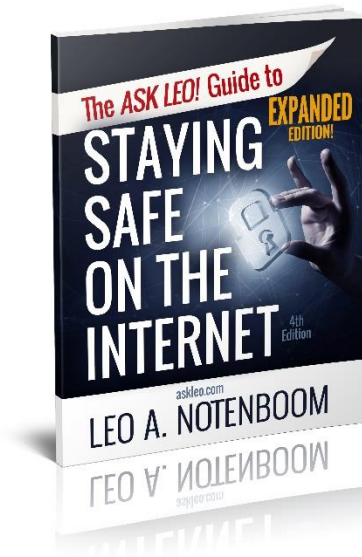
## Sharing this Document

This free edition of *The Ask Leo! Guide to Staying Safe On The Internet* may be shared with others with one simple rule:

You can't change it in any way.

## 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\*](#).

Get your copy now!

## More Ask Leo! Books

If you found this book helpful, check out my growing library of books at <https://store.askleo.com>.

The list is always growing, but here are a few of my most popular titles.



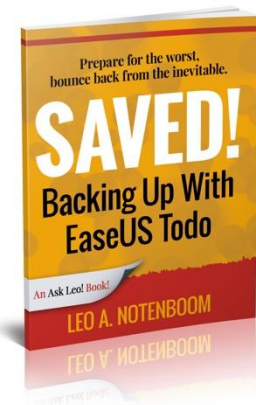
## Saved! Backing Up with EaseUS Todo

*Saved! – Backing Up with EaseUS Todo* will show you – *step by step* – how to back up your Windows computer using this powerful and reliable backup software.

You'll feel confident, and safe.

Ready for anything.

Start backing up *now*!



### How To...

*Saved! – Backing Up with EaseUS Todo* isn't a boring reference manual full of obscure details you'll never use. Instead, it's all about *How To*:

- *How to* download and install EaseUS Todo
- *How to* create an image backup
- *How to* create an emergency disk
- *How to* restore an image backup
- *How to* schedule backups
- *How to* keep from running out of space
- *How to* test your backups

and more. Everything you need to protect your computer and your data.

[Saved! Backing Up With EaseUS Todo](#)

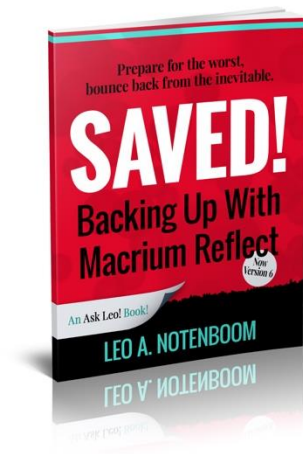
## Saved! Backing Up with Macrium Reflect

Prepare for the worst – Bounce back from the inevitable

*Now Updated for Macrium Reflect Version 6*

- ◆ Never lose data again!
- ◆ Recover quickly from even the worst malware
- ◆ Get back that file you accidentally deleted

[Saved! Backing Up with Macrium Reflect](#)

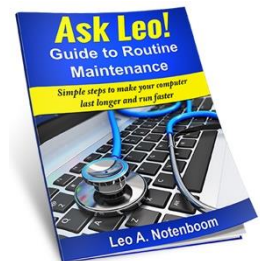


## The Ask Leo! Guide to Routine Maintenance

*Make Your Computer Last*

- ◆ Keep it running longer.
- ◆ Speed it up.
- ◆ Free up space.
- ◆ Save money.

[The Ask Leo! Guide to Routine Maintenance](#)

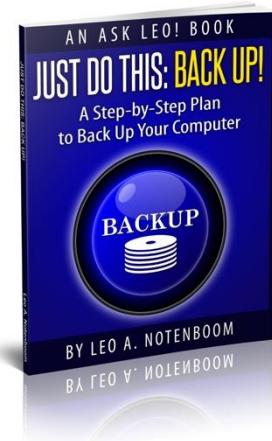


## Just Do This: Back Up!

Instead of giving option after confusing option, Just Do This: Back Up outlines a step by step arrangement for backing up your desktop or laptop PC that just works. Follow these instructions, watch the videos that are included with the book, and you'll be backed up.

You'll be protected against everything from hardware failure to malware infestation and all the minor-to-major inconveniences in between.

Backups are important. So important that if you do nothing else... **Just Do This: Back Up!**



You'll find these and many more popular titles at [The Ask Leo! Store](#).