

The
Ask Leo!
Guide to

**STAYING SAFE ON
THE INTERNET**



LEO NOTENBOOM

The Ask Leo! Guide to Staying Safe on the Internet

**Keep
Your Computer,
Your Data,
And
Yourself
Safe on the Internet**

Version 2.0

by

Leo A. Notenboom

An Ask Leo!® ebook

ISBN: 978-1-937018-23-8 (PDF)

ISBN: 978-1-937018-24-5 (ebook)

ISBN: 978-1-937018-25-2 (paperback)

Copyright © 2014

Contents

Making Technology Work for Everyone	7
What We'll Cover	7
Be Sure To Register	9
Protect Your Data	10
Back it up, back it up, back it up	10
The threats backups address	11
Two types of backups	11
Two methods of backing up	12
Backup locations	13
How do you back up?	13
A suggested backup plan	14
Bonus	15
Protect Your Computer	16
The first line of defense: firewalls	16
What's a firewall?	16
Network-based threats	17
Two basic types of firewalls	18
Choosing and setting up a firewall	19
What firewalls can't do	20
More information	21
Dealing with malware	21
Perplexing terminology	21
A closer look at the malware race: it's partly just luck	23
My general software recommendation	24
How the software works	29
Removing malware	30
PUPS	39

<u>Uninstall the somewhat well-behaved</u>	<u>40</u>
<u>Run Malwarebytes</u>	<u>40</u>
<u>Run AdwCleaner</u>	<u>41</u>
<u>The ultimate removal</u>	<u>42</u>
<u>Prevention</u>	<u>42</u>
<u>Keeping current</u>	<u>43</u>
<u>Updating Windows</u>	<u>44</u>
<u>Windows XP</u>	<u>47</u>
<u>Keeping applications up to date</u>	<u>48</u>
<u>Updating Drivers</u>	<u>49</u>
<u>When updates go wrong</u>	<u>50</u>
<u>Protect Your Laptop</u>	<u>51</u>
<u>The open Wi-Fi problem</u>	<u>52</u>
<u>Turn on the firewall</u>	<u>53</u>
<u>Secure your desktop email program</u>	<u>53</u>
<u>Secure your web-based email</u>	<u>54</u>
<u>Secure all your other online accounts</u>	<u>55</u>
<u>Use a VPN</u>	<u>55</u>
<u>Use different passwords</u>	<u>55</u>
<u>Consider not using free Wi-Fi at all</u>	<u>56</u>
<u>Safety at hotels</u>	<u>57</u>
<u>Computer theft</u>	<u>60</u>
<u>It's more than travel</u>	<u>60</u>
<u>Data loss</u>	<u>61</u>
<u>Mobile devices</u>	<u>62</u>
<u>Theft and loss</u>	<u>62</u>
<u>Protect Your Online World</u>	<u>64</u>
<u>The Cloud: online services</u>	<u>64</u>
<u>Protecting your data online</u>	<u>65</u>

<u>What is the cloud?</u>	<u>66</u>
<u>Online service disasters</u>	<u>66</u>
<u>Backing up email</u>	<u>67</u>
<u>How to back up your email</u>	<u>68</u>
<u>Backing up email: issues</u>	<u>69</u>
<u>Backing Up Your Photos and Videos</u>	<u>69</u>
<u>Backing up your digital camera</u>	<u>70</u>
<u>Backing up your smartphone's pictures and videos</u>	<u>71</u>
<u>Backing up other online photos</u>	<u>72</u>
<u>Backing up photos online</u>	<u>73</u>
<u>Save the raw files</u>	<u>74</u>
<u>A note about "sensitive" photos</u>	<u>74</u>
<u>Backing up your websites</u>	<u>75</u>
<u>Don't rely on the web host</u>	<u>76</u>
<u>Two kinds of web sites</u>	<u>76</u>
<u>What I do</u>	<u>78</u>
<u>Choose Appropriate Passwords & More</u>	<u>79</u>
<u>Strong passwords</u>	<u>79</u>
<u>Using different passwords</u>	<u>85</u>
<u>Managing lots of passwords</u>	<u>87</u>
<u>Two-factor Authentication</u>	<u>94</u>
<u>Set Up Recovery Information</u>	<u>99</u>
<u>The most common reason account recovery fails</u>	<u>99</u>
<u>Alternate email addresses</u>	<u>100</u>
<u>The conundrum of the phone</u>	<u>100</u>
<u>Losing your account in one easy step</u>	<u>101</u>
<u>Do this NOW</u>	<u>102</u>
<u>Recover A Hacked Account</u>	<u>102</u>
<u>1. Recover your account</u>	<u>103</u>

2. Change your password	104
3. Change Your Recovery Information	104
4. Check Related Accounts	105
5. Let Your Contacts Know	106
6. Start Backing Up	106
7. Learn from the experience	107
8. If You're Not Sure, Get Help	108
Protect Yourself	109
Why you need malware scanners	109
Why?	111
Use Your Common Sense	111
If it sounds too good to be true...	111
If it ain't broke, don't fix it	112
Free is never free	113
Read what's in front of you	114
Don't believe everything you read	115
Above all, be skeptical	115
Do your research!	116
Learn who to trust	118
A good download site is hard to find	120
Phish or cut bait	122
Conclusion: it's not your fault (but it is your responsibility)	126
Afterword	127
The Ask Leo! Newsletter	128
Register Your Book!	129
About the Author	130
Feedback, Questions and Contacting Leo	132
Copyright & Administrivia	132
Sharing this Document	133

Making Technology Work for Everyone

I believe personal technology is key to humanity's future. It has an amazing potential to empower individuals.

But it can also frustrate and intimidate.

I want to make technology work for you.

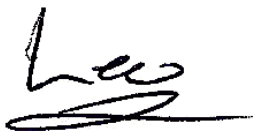
I want to replace that *frustration* and *intimidation* with the *amazement* and *wonder* that I feel every day.

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

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

I just want it to work, for you.

That's why Ask Leo! exists.



Leo A. Notenboom

<http://askleo.com>

<http://askleobooks.com>

What We'll Cover

The very concept of "Internet Safety" seems like an oxymoron - the words just seem like opposites.

Not a day goes by where we don't hear about everything from hacked accounts and computers, to viruses, spyware and other forms of malware to large data breaches that threaten our online information.

“Internet Safety” indeed.

In this book I'm going to cover the the things you must do, the software you must run and the concepts you need to be aware of - to keep your computer and your data safe as you use the internet.

It's really not that hard, and once things are in place it's not even that time consuming.

But it is necessary.

I've divided the book in to several sections:

Protect Your Data: Anyone that knows me knows I talk a lot about backing up. Protecting your data - be it on-line or off - is a key part of making any problems that arise no more than annoyance rather than the disaster we so often hear about.

Protect Your Computer: Your computer is a target for a wide variety of malware including viruses, spyware, and the ironically named “Potentially Unwanted Program” (there's nothing “potentially” about it). I'll cover the tools and techniques you need to keep your machine safe.

Protect Your Laptop: Portable computers carry with them enough additional risks that I've dedicated a section to dealing with the potential for theft, eavesdropping and more.

Protect Your Online World: In recent years much of what we do and keep has moved online, or into “the cloud”. With that move come additional and unique threats that I'll show you how to protect yourself against.

Protect Yourself: There's no software, no device, no *anything* that can protect you from yourself. I'll cover the things to look for when the bad guys try to fool you into installing malware, handing over sensitive data, or just generally try and manipulate you into doing something you didn't really want to do.

Naturally things don't always align themselves so neatly into those five categories, so you'll certainly see a lot of cross referencing and related topics throughout.

I do want to be clear about a couple of things that this books is not about:

- **Spam** - While most definitely annoying, technically spam doesn't threaten your computer or your information's safety, so "protection" doesn't really apply. However I do address the special case of phishing which often arrives as spam.
- **Mobile Devices** - While the concepts apply across all computing devices this book is targeted specifically at traditional computers - desktops, laptops, PCs, Macs and similar. Much of the content is still quite relevant, I just don't have recommendations for software or techniques that would be specific to Android / iPhone / Windows Phone / etc. - based devices.
- With that, let's turn "Internet Safety" from an oxymoron to a statement of fact.

Be Sure To Register

Your purchase of this book entitles you to several additional free bonuses:

- All available digital formats of the book as direct downloads, so that regardless of which version you purchase you can enjoy this book on the digital device of your choice.
- Updates, errata, and prioritized Q&A.
- Any additional bonuses that might be made available.

You'll find the information that you need to register in a chapter called "Register Your Book!" near the end of the book. Once you register you'll have access to a web site specifically for this book that will list all available bonuses and updates.

Protect Your Data



Back it up, back it up, back it up

What's the one thing on your computer that can't be replaced?

Your data.

Programs can be replaced; settings can be reconfigured; even entire machines can be replaced, should the absolute worst happen.

But if your data is lost - say your precious photographs, important emails or other information is lost - then without preparation it's lost *forever*.

Ask Leo! readers are probably tired of hearing me say it, but there's a very simple rule:

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

Yes, backups are the solution for just about every problem, and that's why it's the first and perhaps most important part of keeping yourself safe online or off.

The threats backups address

Backups are one of the single most important ways you can protect yourself, not just from data loss, but also from a variety of issues that can threaten your technology.

- Computer crash? Restore your data from a backup.
- Massive malware infection? Take your computer back to the past by restoring a backup image taken prior to the infestation.
- Online account breach? By having that account's information duplicated elsewhere you lose nothing.

Backups really are the silver bullet of computing and online technology.

Two types of backups

Let's look at two different types of backups:

- Backing up your computer
- Backing up your online life

Backing up is nothing more than making a copy of data and/or program files and then keeping that copy in a safe place.

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. In fact, that leads to one of my most important rules of thumb:

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

I occasionally run across folks who misunderstand the concept. After copying their information to their backup drive, they delete the original, leaving only a single copy 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 goal of a backup is also simple: if something happens to your computer so that you can't retrieve your information from it (which happens more often than people realize) or you somehow otherwise lose access to your data, then you can get the information from the backup copies.

The concept is simple. Where it starts to seem complicated is when you look at all of the options relating to how much to back up, how often, and what tools to use to make sure that it happens regularly.

Two methods of backing up

Backups typically take one of two forms:

- **Copying your data.** If you copy pictures off of your digital camera and then immediately burn those pictures to a CD for safekeeping without deleting them from either the camera or the computer you copied them to, you've backed them up. Similarly, if you regularly take the contents of your "My Documents" folder tree and copy it to another machine or burn it to CD, that's one form of backing those files up. They're safely stored in another location in addition to the original.
- **Imaging your system.** Rather than backing up only this-and-that, hoping you've actually remembered to include everything you might need in case of a disaster, this approach makes a copy of *absolutely everything*: your data, your programs, your settings - even the operating system itself.

Both types of backups share a common characteristic. Whatever they backup, be it specific files and folders or absolutely everything, they do so by a) making a copy, and then b) placing that copy somewhere else.

If your data is in only one place, (meaning that there are no additional 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 the backup lives, the more you are protected from various types of disasters.

- If the backup is on the same hard disk as the data, and the hard disk dies, then you could lose your data *and* your backup.
- If the backup is on a different hard disk, but inside the same computer, then you could lose your data and your backup if something happens to the computer that causes both hard disks to be harmed (or stolen).
- If the backup is on an external hard disk but connected to the same computer, then 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, then a network problem or malware on your local network could start deleting files and you could lose your original data and your backup.
- If the backup is burned to a CD or DVD, but kept in the same physical location, then you could lose your data and your backup if that location suffers a physical catastrophe (such as a fire or flood). This is true of any solution kept in the same place as your original data.

That's scary stuff, but you get the idea. The closer your backup is to the original data, the greater the possibility you could lose both at once. It doesn't happen often, but it can. So, make a copy of your data and store it in a safe place away from your computer - perhaps by using an online backup service, perhaps by swapping backup disks with a trusted neighbor.

How do you back up?