The Ask Leo Guide to Staying Safe on the Internet

EXPANDED Edition

4th Edition

by

Leo A. Notenboom

http://askleo.com


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

Part 1: Protect Yourself

- It Pays to Be Skeptical .............................................................................. 3
- Just What Is Common Sense? ................................................................. 7
- Stop Spreading Manure ........................................................................... 14

Part 2: Protect Your Data

- How Do I Back Up My Computer? ......................................................... 20
- What Backup Program Should I Use? .................................................... 27
- Can’t I Just Copy Everything Instead of Using a Back-up Program? .......... 31
- How Do I Test My Backups? ................................................................. 35
- Four Important Rules to Safely use Cloud Storage as Cloud Backup .... 38

Part 3: Protect Your Computer

- Protecting with Firewalls ....................................................................... 41
- Do I Need a Firewall, and If So, What Kind? ......................................... 41
- Is an Outbound Firewall Needed? .......................................................... 46
- How Do I Secure My Router? ............................................................... 50

Part 4: Protect Your Laptop

- How Do I Use an Open Wi-Fi Hotspot Safely? .................................... 110
- Can Hotel Internet Traffic Be Sniffed? ................................................... 116
- How Can I Keep Data on My Laptop Secure? ......................................... 119
- My Password-protected Computer was Stolen. What Files Can the Thieves See? ...... 123

Part 5: Protect Your Online World .......................................................... 128
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: A Freebie for You

You're looking at the EXPANDED 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.

• The FREE version of The Ask Leo! Guide to Staying Safe on the Internet. A shorter, more compact version of this book that you can share with your friends and family.
• 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 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.¹

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

¹ 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

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.”

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.

---

2 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.³

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.

³ That’s one reason I took on 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\(^4\) 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\(^5\) 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

\(^4\) 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.

\(^5\) 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.6

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

6 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.
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 and dozens of other media sites.

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.

We need to learn to draw our own conclusions.

______________________________

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