BOB THE TECH GUY

The Online Security Guide

How to Avoid Hackers & Scammers



Clickware

Table of Contents

Technology - Not Everyone "Gets It" 1

Data Breaches Are Here To Stay 3

The Moment I Knew I Had To Do "Something" 5

Start at the Beginning: Password Security 7

- Step 1 - Choose a Secure Password 7
- Step 2 – Use a Password Manager 9
- Step 3 – Use Two-Factor Authentication 11
- Step 4 – Security Questions and Answers 12
- Step 5 – Separate Password Recovery Email Address 13

Beyond Passwords: Antivirus/Antimalware 14

Phishing – Don't Fall For It! 15

- The Email Asks To Confirm Personal Information 16
- The Email or Web URL Doesn't Seem Right 17
- The Email is Poorly Written 18
- The Email Has an Attachment 19
- The Email Uses Threats or Scare Tactics to Pressure You into Action 20

Protect Your Mobile Phone 21

- Set a Passcode 21

Protect Your Cellular Account 22
Back Up Your Data 23
Local Backups 24
Local Backup Software 24
Offsite Backups 25
Beware of Technical Support and Sweepstakes Scams 27
Technical Support Scams 27
Extra Credit – More Privacy Protection 29
Ad Blockers and Anti-Tracking Browser Plug-Ins 30
Ad Blockers 30
Anti-Tracking Plug-Ins 31
Disable Flash 33
There is No Such Thing as “Perfect” 34

Technology - Not Everyone "Gets It"

Are you (or your parents or grandparents) just plain curious? Do any of you click on email attachments or online links that they shouldn't? It's time that you help educate yourself and your loved ones in how the real Internet World works and give and yourself peace of mind.

It's not your fault - you have good intentions. But hey, let’s face it most of us grew up reading printed magazines and newspapers that were printed daily.

We used rotary phones, sent handwritten letters through the post office and read hardback books. We listened to records, passed paper notes in class, and rushed home to catch their favorite shows on live TV.

In short – most of us grew up in a world that was totally different than the always-on, time-shifted, interconnected world we live in today. As a consequence, most of us may not be the most "technically literate" people on the face of the earth.

That's where I can help.

How do I know? Because I'm "that guy". You know, the person that everyone in the extended family calls when they are looking to buy a new computer or "can't get their

printer to print", or get advice on anything do to with "technology".

I've been involved with technology for over 25 years. It all started when I saw the 1983 movie "War Games" wrote my first gaming program on an Apple II in Applesoft BASIC - that I learned from the Apple II manual (here's a text version if you're insane))

From there, I my life journey was a *slightly twisted* - I started a graphic design business, did overnight pen-and-ink artwork for the aerospace industry, co-founded Day of the Child - a international day to raise the awareness of Child Abuse & Neglect, was co-founder of an Adverting Agency doing print and radio nationally - and finally, co-founding my first software company - Working Solutionz Software.

I went on to be the founder of two more software companies and I have created custom software for hundreds of companies (Volvo, Disney, E! Entertainment Television, Apple, etc.)

I was an avid blogger back in the early days of the interwebs (if you want a laugh - check out https://bobcusick.blogspot.com/) - and through it all - one thing has remained the same: my "job" is my hobby as well: I just love all facets of technology - and, above all, I love to help people solve problems.

I'm guessing you're the same type of person.

Maybe you're tired of worrying whether or not you (or your loved ones) will click on something that will infect their computer. Maybe it's too late - and someone you love has been hacked or had their identity compromised. Maybe you're not sure how to protect yourself and others online.

Even if you don't fully understand technology or you just plain don't know where to start – there is no need to worry! I'm here to help you out with step-by-step instructions.

Data Breaches Are Here To Stay

It's the one thing that all of us in our interconnected society dread - being "hacked." It seems like data breaches and hackers stealing personal information and data "leaks" happen more and more frequently.

Here's just some of the craziest ones:

- Adobe - 2013: Personal information of 2.9 million accounts was stolen (logins, passwords, names, credit card numbers and expiration dates);
- Sony - 2011: The personal data of 77 million users which was leaked, and in 2014 100 terabytes of data including large quantities of confidential information such as film scripts, compromising emails and personal data of 47 000 employees

(names, addresses, emails, social insurance numbers, salaries etc.) was stolen via malware;

- Target - 2013: Data from 110 million customers was hijacked - including banking data of 40 million customers and personal data (names, postal addresses, telephone numbers, and email addresses) of another 70 million customers;
- Equifax - 2017: Hackers store the personal data (names, birthdates, social insurance numbers, driver's license numbers) of 143 million American, Canadian and British customers as well as 200,000 credit card numbers;
- Marriott - 2018: Breach of personal information of 500 milllion guests who booked stays before Sept 10, 2018. Of those, 327 million records included payment information, names, mailing addresses, phone numbers, email addresses, passport numbers, and even details about the Starwood Preferred Guest (SPG);
- Yahoo - 2018: Yahoo! announced it had suffered a cyber-attack in 2014 that affected 500 million user accounts constituting the largest massive hacking of individual data directed against a single company. Names, dates of birth, telephone numbers and passwords. THEN, in March, 2018 - they admitted that 3 billion user accounts had been hacked in 2013
- Facebook - 2018: Hackers got the data on over 30 million users - including the search history of 14 million users;
- British Airways - 2018: 500,000 customers names, addresses, email addresses, card numbers, expiration dates, and card verification value (CVV) numbers;

And on, and on, and on. That's not mentioning MySpace (360 million), Adult FriendFinder (214 million), EBay (145 million), LinkedIn (100 million), AOL (92 million), JP Morgan Chase (83 million), Tumblr (65 millioin), Uber (57 million) or Home Depot (53 million).

Those numbers are mind-boggling. It's really tough to wrap your head around. There's even a website (https://haveibeenpwned.com) that contains over 7 BILLION compromised email addresses and accounts - so you can check if your email has been swept up by any of the (known) hacks.

The Moment I Knew I Had To Do "Something"

I hope it never happens to you or anyone you love - but there was one moment when hacking "got real" for me. One day my mom sent me a text (a miracle in itself!) - saying:

"I'm sorry Bob your Social Security # may be compromised! I got hacked!!"

What the actual hell? So, being the normally calm, level-headed "tech guy" I replied:

"How do you know you were hacked?"

To which she replied:

"I got the red screen and told to call a #. Stupid me called it. Told me I was infected with Trojan. And they flashed SS#s with your names, they also flashed credit card #s. They wanted $550/yr to take care of the trojan. The police just left. I already called my bank."

Well, crap.

It's one thing if you personally have had information that was compromised - chances are that you have taken precautions from that happening again (right?). But WHEN (not IF) you get that phone call from your loved one saying "I think I've been hacked" - that sense of fight-or-flight will kick in.

I can see you nodding your head in agreement - but you may be asking yourself "yeah, but what can I do?"

You, as an individual user (or person wanting to help your loved ones), can't do anything to prevent your email provider, cell phone provider, social media site, hotel operator, airline or banking institution from getting hacked.

But there are things you CAN do to help minimize the risks of being hacked as well as some tips and tricks to

recognizing risky links and email phishing attacks that have become all-too-common.

Start at the Beginning: Password Security

Most of us like to think we're pretty savvy in the ways of technology and cybersecurity, but research has shown that 59% of people use the same password for most websites.

We all have too many passwords to remember, which is why 59% of us just reuse the same ones over and over. If you or your loved one is guilty of this **STOP IT** today.

It's never a good idea to use the same password for multiple sites because if a hacker gets a hold of your username and password – they could potentially have access to all your accounts!

OK – so now that we know we shouldn't use the same password everywhere – let's talk about how to setup your passwords and security questions so that it makes it harder for hackers to get to your information.

Step 1 - Choose a Secure Password

A secure password is simply a password that is easy for you to remember – but hard for anyone to guess.

Although it's tempting – using pieces of common information in a password is a very bad idea. Avoid using things like your name, your child's name, your house number, birthday, anniversary, pet names or other obvious choices for your password.

Why? Because I'll bet

Your password should be at least ten characters long and not a normally spelled word from the dictionary (hackers use "brute force" attacks that try to gain access to an account using every word in the dictionary).

Ideally, each password would be totally random – something like: **g@$K9xbDHd*£9#!** Now, I know what you're thinking – "There's NO WAY I could ever remember something like that!" – And you're probably right!

Instead, you could use something complicated like a code, or choose an original statement. A long string of unrelated words mixed in with numbers like "SuperSimpleKeepsMeSafe" is a definite step up from your first name followed by the month and day of your anniversary or kid's birthday.

You should also use numbers and symbols in place of letters – but use it sparingly so it's not too obvious. For example, changing "SuperSimpleKeepsMeSafe" to

“Super$impleKe3psMeS@fe!” is a much more secure password and will be harder for hackers to guess.

Still, using strong passwords can be a hassle – especially if you have to come up with multiple passwords for multiple sites. That leads us to Step #2 – using a password manager to keep track of all our unique passwords.

Step 2 – Use a Password Manager

If the prospect of coming up with (and remembering!) complicated passwords sounds impossible – don’t worry – its technology to the rescue (!) – In the form of a password manager.

Password managers are applications/services that help you store and organize your passwords so that you only need to log in once with that password. You can change your passwords, fill out forms, and save credit card information on without having to remember each password individually.

Typically, you either download an application to your computer or install a browser plug-in, and create (and remember) one master password. The password manager will then keep track of the sites you visit, and will automatically fill in the password for you.

It's easy to then update your passwords on each site – the password manager will even suggest a strong, random password – and store it for you automatically.

If you have more than one device that you use to access online accounts (and who doesn't these days?) – the password managers can be installed on each device (phone, laptop, desktop, tablets) and you still only have to ever remember a single password.

As you update your passwords – these password managers will automatically synchronize any changes between all your devices – automatically!

Here are a couple of very good password management tools that are inexpensive and painless to setup and use: LastPass and 1Password.

I would recommend getting the "Family" plan (6 users for LastPass - $4/month and 5 users for 1Password - $4.99/month) because if worst comes to worst - at least you can recover a loved-one's passwords for them.

You should make sure that if you're setting up a password manager either for yourself or a loved one – make sure you write down their master password and keep it in a safe place!

Step 3 – Use Two-Factor Authentication

Two-factor authentication is a just fancy way of a website asking, "Are you who you say you are?" It works like this: when you log in to a site that supports two-factor authentication, you'll receive a text message or an e-mail with an additional code. Sometimes you can also download a special app that generates this code on your phone.

The bottom line is: no one will be able to log into your account unless they enter that code into the client (including you!). In addition to adding an additional layer of protection, receiving a two-factor authentication code when you're not trying to log in is also a great way to know someone's trying to hack you!

Here's some links that will allow you to setup two-factor authentication on popular social media services:

- Google
- Facebook
- Instagram
- Twitter
- LinkedIn
- Pinterest
- Snapchat
- Dropbox

Step 4 – Security Questions and Answers

Many systems ask their users to create a security question which can be answered if a password needs to be reset or hacking has been detected (like most banking sites).

Choose your security questions and answers carefully. Try not to be so obvious – or even truthful - in your answers. It will be more secure for you to use incorrect answers to your questions, making them harder for even someone who knows you well to figure out.

For example, if the question is your first car model, answer with "BlueAnimalsAreMyFavorite". If possible, add spaces to your answer. For example: “Blue Animals Are My Favorite”.

If the question is your mother's maiden name, don't use your mother's maiden name as the answer. Your mother's maiden name you’re your first car, or your kindergarten teacher, or your first pet’s name, etc.

Chances are – all of these pieces of information could easily acquire through social media, social engineering, stolen records, public records, malware, easily guessed or many other methods.

If the service lets you – consider using a nonsense string of words and numbers for ALL the answers (like when we talked about generating secure passwords earlier).

Step 5 – Separate Password Recovery Email Address

Since you're now using two-factor authentication on all your accounts (right?) – you should consider setting up a separate email account that is only used for password recovery.

This is a NEW email address you setup ONLY for password recovery. You don't use it for ANY other purpose. No sign-ups, no conversations with your friends – nothing.

Then you go back into each of your services and specify that new email address as the password recovery address. That way – if your main email gets hacked – the hacker can't just reset all your passwords and take control of your entire online life!

Here's a true story:

Say you have an Apple ID and make use of their free email account. Now let's also assume you have a Gmail account as well – and you specified your Apple email as the password recovery email address.

All a hacker needs to do is to go on Apple's site – open a chat window and convince the tech that they need to reset the password on their account. The tech would then try to ask some security questions (which the hacker can guess from your social media posts).

When that fails – the hacker explains that the tech needs to send the password reset email to HIS email using the excuse “my email was hacked.”

Once he resets the apple account, the hacker can now go to Google and use the “I forgot my email” link to have Google send the compromised Apple account a link to reset the Google account.

Done. Now the hacker has access to not only the Apple email account but all of your Gmail, Google Docs, Google Sheets, Google Voice, etc.

Beyond Passwords: Antivirus/Antimalware

Yes, you've heard this before. And it’s still true. You really, really need to have an antivirus program installed on your computer.

If you run Windows 10, you already have one (Microsoft implemented its own antivirus engine, called Defender), but according to experts, there are some advantages to running a third-party one.

If you have a Mac – you may think that you’re immune from viruses and malware – you’re not. While the MacOS is generally less susceptible to viruses – it’s not 100% safe.

You really can't go wrong in having an "extra layer" of protection from all the *viruses* (can delete files on your computer) *malware* (spies on you and can mess up the way your computer works) and *ransomware* (a nasty program that locks all the files on your computer until you pay a fee).

Here are 4 anti-virus providers that have cross-platform (both Mac and Windows) offerings – prices are per year (things change - these may not be the latest prices):

Kaspersky - $29.99 for 3 devices, $39.99 for 5 devices

Bitdefender - $25.99 for 1 device, $39.98 for 3 devices

McAfee - $24.99 for 1 device, $39.99 for 5 devices

Webroot - $18.99 for 1 device, $29.99 for 5 devices

Sophos Home - $45.00 for up to 10 devices

Phishing – Don't Fall For It!

Phishing (pronounced "fishing") is a set of taticts that scammers and hackers use to fool you into giving up your personal information either via email or on the phone. Your best defense against becoming a victim of a phishing attack is your own common sense. Hackers use all kinds of tricks in order to get you to reveal your passwords or to just plain separate you from your money!

There are some common tactics – so if you see one or more of these in an email – or a phone call – DELETE the email or HANG UP the phone!

- Asking to confirm personal information
- The email address or the link address doesn't look right
- It's poorly written
- There is any kind of attachment
- The message is meant to scare you into taking action right away

The Email Asks To Confirm Personal Information

Your bank **is not** going to send you an email telling you that you need to log in and update your account information. EBay or Amazon **will not ever** send you an email asking you to change your password by providing a link in an email.

If you do want to change your password (and you should – once you get your Password Manager!) – always login directly on the website and change your password there.

Your personal information is like money. It's valuable and you should take care in protecting it.

The Email or Web URL Doesn't Seem Right

You may get an email from a bank, social media site, or ecommerce website that looks authentic. Hackers and scammers go to extreme lengths to imitate the style of legitimate company emails.

One sure tip-off that the email is not authentic or the link they are asking you to click is to a potentially malicious site – is all in the domain name.

For example – bankofamerica.com is a legitimate website. If you go to that URL – you will see that it is the official site of Bank of America – and you can expect communications that come from them to have "@bankofamerica.com" or "@alerts.bankofamerica.com" as the "from" email.

Likewise – if there are any links in the email (or a button that says something like "View Account" – NEVER JUST CLICK IT. Instead, if you hover your mouse over the link (or button) it will display the full URL that you will be taken to.

Make sure that this URL matches the domain. Using our Bank of America example – any link should contain: https://bankofamerica.com/xxxx/xxx. Sometimes there will be a subdomain at the start – like this: https://ealerts.bankofamerica.com/xx/xx. The key thing to look for is that "bankofamerica.com" is the actual site you're directed to.

Scammers and hackers are very good at trying to fool you. Sometimes they will change subtle letters in the URL so that at first glance, everything looks legitimate. For example:

- bankfamerica.com (missing the “o”)
- bankofamerica.cc (using “.cc” and not “.com”)
- bankofameria.com (missing the “c”)
- bankofamerica.5478j.com (link is pointed at 5478j.com)

Do not reply or click on any of links. If you think it’s a real request – contact the organization directly – and don’t use any of the communication methods outlined in the email (phone, clickable link, button, etc).

When in doubt – throw it out!

The Email is Poorly Written

Legitimate companies go through great pains to ensure that their emails are free from typos, misspellings and include proper grammar.

If you have received an unexpected email from a company, and it is riddled with mistakes, this can be a strong indicator it is actually a phishing email – trying to get you to give up your personal information.

The Email Has an Attachment

There are **exactly zero** legitimate companies that will send you a file attached to an email. Likewise – even if someone you know sends you an unexpected email with an attachment – DO NOT CLICK IT unless you verify with that person that they did, indeed send it.

The reason is because your friend's email account may have been attacked – and the scammer or hacker is targeting everyone in their contact list.

This is especially true if it's a "joke" email with an attachment, or it's a "here's the file you requested" email. Even the name of the attachment should be a tip off. Things like "document.zip" or "jokes.pdf" or "finances.xls" can really be any type of file.

The attachment could contain a malicious URL or trojan, leading to the installation of a virus or malware on your PC or network. Even if you think an attachment is the real deal, it's a good practice to always scan it first using your antivirus software.

When in doubt – throw it out!

The Email Uses Threats or Scare Tactics to Pressure You into Action

The IRS is not going to call you up and tell you they have a warrant for your arrest and are coming to haul you off the prison unless you give them a credit card number right now to pay the back taxes you owe.

Likewise, if the email subject contains some scary language, has words in ALL CAPITALS or contains one or more exclamation points – you should be wary. For example emails with these type of subjects: "Your Recent Payment was DECLINED!", or "Your Shipment Could Not Be Delivered", or "Warning: Your Computer Has a Virus", or "Your IMMEDIATE Response is REQUIRED!" – usually indicate that the email is either a scam or a phishing attempt.

The best advice is "When in doubt – throw it out". If something doesn't look right – or seems too good to be true – or contains spelling mistakes - or if you just have a "wonky" feeling – it's best to just delete the email or HANG UP the phone!

Protect Your Mobile Phone

There are some easy steps you can take to help ensure that your mobile phone is hack-resistant – and the best part is that it won't cost you a dime!

Set a Passcode

One of the biggest mobile threats is someone who has physical access to your phone and can unlock it. Now I'm sure that you have locked your phone with a passcode – right? If not – please do this **NOW**.

Your mobile phone security is only as good as your passcode: If at all possible, avoid giving out your code or password, and avoid using easily guessed passcodes such as your birthday or address.

Even simple passcodes and passwords are great to stop pickpockets or street thieves. Use alphanumeric passwords of at least 7 characters to unlock your phone.

Now I understand that inputting 7 or more digits every time you need to read a text may sounds totally annoying, but modern smartphones are armed with fingerprint or facial recognition technologies that can make that login process a lot easier.

Unless you're worried that the authorities may legally coerce you to unlock your phone with something like TouchID or FaceID, that's the best way to go.

Protect Your Cellular Account

As I said before, you can't stop your cellular provider from being hacked. But you can make it a bit harder for hackers to impersonate you with gullible tech support employees.

The solution is really easy – set up a secondary password (or passcode) that is required when you call your provider. This will help ensure that no one makes any changes to your account without you knowing about it.

Here's some links that give you instructions on how to work with your carrier to setup this extra layer of protection:

- Verizon
- AT&T
- T-Mobile
- Sprint

If you want to security a step further - you can remove your real mobile number from any of your sensitive online accounts and substitute a free VoIP (Voice over Internet Protocol – basically a call that gets transferred to your phone over the Internet). You can use a FREE Google Voice number – or a FREE Skype number.

This allows you to change the phone number that the calls are forwarded to. This comes in really handy if you ever have your phone stolen or lost and get a new mobile number.

Rather than changing your phone number in all your different accounts – all you have to do is change the ONE number that all the calls are forwarded to.

Back Up Your Data

Nowadays a lot of the work we create is stored "in the cloud" – meaning we access it via a web browser so it's not stored on our local computer.

However, if you DO store ANYTHING on your local computer – you need to back it up. There are a number of reasons you need a backup strategy:

- 100% of hard drives WILL FAIL at some point;
- You could be a victim of ransomware and your local files get locked or erased;
- There is a flood, fire, tornado or other disaster that destroys or damages your computer;

Ideally, you should have two backups – one that is "local" and one that is "offsite".

Local Backups

A “local” backup is one where you have either another external hard drive or USB stick that you backup your data to. USB sticks are small and inexpensive and have more than enough capacity to store all of your documents.

USB sticks are a very inexpensive option for local backups. They are solid state – which means there are no moving parts – so they tend to last a very long time.

Even if you have a TON of photos and documents - you can get a 128 gigabyte USB stick for about $25 at your local Best Buy, computer store or Amazon.

That should be more than enough storage for most people. If you need (or want) more storage – then an external hard drive is a must. You can pick up a 1 terabyte (that’s 1,000 gigabytes!) hard drive for around $50 on Amazon. I personally use the Western Digital “My Passport” External hard drive – they are inexpensive and work with both my Macs and my PCs.

Local Backup Software

If you don’t have that many files – or the file you have don’t change (think photos or music) – it’s easy enough to manually drag them to your USB stick or external hard drive.

If you're using a Mac – then you have great built-in backup software called "Time Machine". Simply hook up your external hard drive, go into the system preferences and choose "Time Machine", choose your external hard drive from the list – and click "Use Backup Disk". Done.

If you're on a PC – running either Windows 7 or Windows 10 (you're probably running Windows 10 if you have a computer that is newer than 4 years old) - select the Start button, then select Control Panel > System and Maintenance > Backup and Restore. If you've never used Windows Backup before, or recently upgraded your version of Windows, select "Set up backup", and then follow the steps in the wizard.

The good news about local backups – is that you have a copy of all of your data. The bad news is – a disaster could wipe out your backups like it could damage your computer.

That's why it's also important to have an "offsite backup."

Offsite Backups

An "offsite backup" is just what it says – it's a copy of your data that is stored at a location that isn't where your physical computer is located.

Back in “good old days” when backups were done on magnetic tape – we would literally drive the day’s backups to another building for storage!

Now that we have the Internet – offsite backups are considerably easier! Just like with creating your local backups there are a number of free (and nearly free) ways to easily backup your stuff.

If you don’t have a lot of files – consider using a free Google account and Google Drive. You can easily drag-and-drop your files from your computer into your browser window and they will be automatically uploaded to Google’s servers.

The only caveat with using Google Drive – is they “only” provide a total of 15 gigabytes of storage – across all of your Google services. If you think you’re going to need more than that – then I recommend going with a commercial software/storage combination.

These two companies offer software that runs on your computer to automatically back up your files to their servers:

- iDrive
- Backblaze

Whether you manually backup your files to the cloud or you use a service – having an offsite backup (especially of your priceless photos!) will help give you peace of mind.

Beware of Technical Support and Sweepstakes Scams

Technical Support Scams

According to the US Federal Trade Commission (FTC) two of the scams that older people fall for are technical support scams and sweepstakes scams.

These fraudsters use both the phone and popup windows in the browser to fool less technically savvy people into paying them for services that you don't need to fix a problem you don't have.

They all have something in common – they will tell you you have something seriously wrong with your computer – like a virus, a Trojan or some malware. They often ask you to give them remote access to your computer and then pretend to run a diagnostic test. DO NOT LET ANYONE REMOTELY ACCESS YOUR COMPUTER.

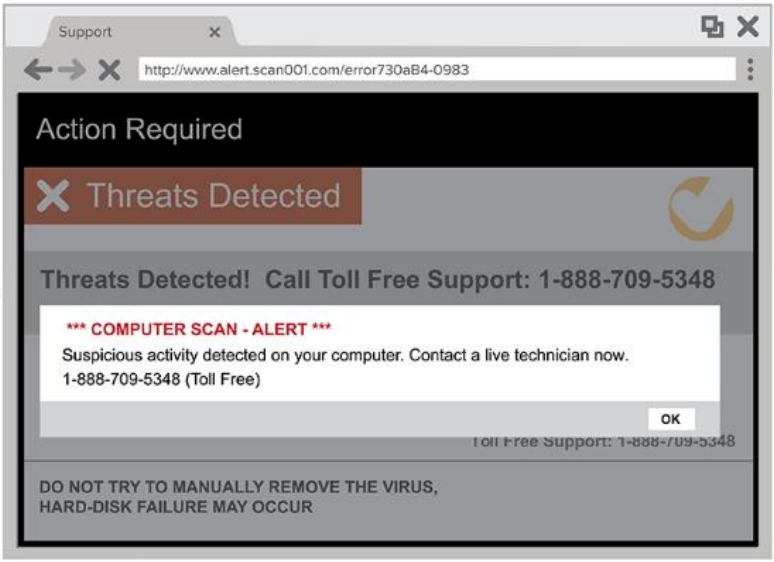
They often ask you to pay by wiring money, putting money on a gift card, prepaid card or cash reload card, or using a

money transfer application because they know those types of payments can be hard to reverse.

If you want to get an idea of how scummy these scammers are - here is an actual recording that took place between an undercover FTC agent and a technical support scammer. It's really eye-opening!

If you get a phone call you didn't expect from someone who says there's a problem with your computer, hang up.

The other way scammers try to lure you in – is via a popup window that appears on your screen. It often can look like an error message or a warning from antivirus software – and it could even have logos of trusted companies or websites. They usually look something like this:



Regardless of the form it takes – all of them warn of a security issue on your computer and tells you to call a phone number to get help. DO NOT CALL THE NUMBER.

Real security warnings and messages will never ask you to call a phone number – and NO ONE besides you "knows" your computer has a problem. No one. Ever.

If you think you're having a problem with your computer – or you see one of these popups - update your security software and run an antivirus scan.

If you need help fixing a problem, go to someone you know and trust. Many software companies offer support online or by phone. Stores that sell computer equipment also offer personal technical support either in-store or by sending a professional to your home.

Extra Credit – More Privacy Protection

If you've made it this far – awesome! I know it can all be a little overwhelming – but once you have it all setup – you can rest easier knowing that you're better protected than most people.

If you really want to protect your privacy – here are a few more tips you may want to consider:

Ad Blockers and Anti-Tracking Browser Plug-Ins

Ad Blockers

Ad and script blockers give you control over your browsing experience. They can block ads on the sites you visit and disable third-party scripts and widgets that send your data to who-knows-where.

However, these tools also have the ability to break the sites you visit – making them unusable unless you unblock them. This is especially true for online news sites like Gizmodo, Lifehacker, etc.

The general rule of thumb is – if you like (and trust) a particular site and want to support them – you'll want to unblock them (I have about 15-20 sites that I've unblocked out of the hundreds of sites I visit per year).

Nevertheless, it's a good idea to install a free ad blocking browser extension.

The granddaddy of them all is called AdBlock Plus. This plugin will work on all popular browsers (Firefox/Chrome/Safari) and blocks banner ads, pop-up ads, rollover ads, and more. It stops you from visiting known malware-hosting domains, and also disables third-party tracking cookies and scripts.

There are a TON of other things that AdBlock Plus can do – here's a great Lifehacker article with the details.

Another contender is called uBlock Origin (NOT the old "uBlock" – confusing, I know). It works in basically the same way as AdBlock Plus but, according to the site –

> *uBlock Origin it is a wide-spectrum blocker -- which happens to be able to function as a mere "ad blocker". The default behavior of uBlock Origin when newly installed is to block ads, trackers and malware sites.*

Because uBlock Origin is more powerful than Adblock Plus – and you can block more types of content – it's less novice-friendly. If you have a bit of a technical bent (or want to learn) then this is another option to consider.

Best of all – both AdBlock Plus and uBlock Origin are free. As in beer.

Anti-Tracking Plug-Ins

It's no secret that there's big money to be made in violating your privacy. All kinds of companies are paying big bucks to learn more about you, and are no shortage of service providers on the web who are more than happy to help.

So - how do you keep as much of your information as possible out of everyone else's hands? Install a free anti-tracking browser plugin.

The adage goes, "If you're not paying for a service, you're the product, not the customer," and it's never been more true. Every day more news breaks about some company that tracks your every move on the web to learn as much about your browsing habits and activities as possible and then sells that information to whomever will pay for it.

Even though there are a ton of plug-ins in this space (and they all do essentially the same thing – stops companies from injecting tracking codes into your browser to track where you go on the Internet.

Like Ablock Plus, the Disconnect private browsing plug-in is available for all popular browsers (Firefox/Chrome/Safari) and protects you from tracking, malware, and malvertising (malware inserted into ads), and offers secure Wi-Fi and bandwidth optimization features that just aren't available in other tools.

And, again, it's FREE. As in beer.

Disable Flash

Adobe Flash is an old technology. It also has more security holes than Swiss cheese. It's not that Flash itself is so bad, it's what hackers do with it.

They can (and have and do and will) create ads that have malicious code in them that can trigger virus, malware or even ransomware – all without you knowing it (until it's too late).

Flash is a dead technology. The whole world has moved on. It had a really great run for 20 years – but in today's world – there is no reason that you need to have Flash installed and potentially exposing you to the dark side of the Internet.

Chris Hoffman from How-To-Geek has an awesome – and easy-to-understand article on how to uninstall and disable Flash in every browser. I recommend that you check it out and get rid of Flash once and for all.

There is No Such Thing as "Perfect"

There is really nothing you can do to **guarantee** that your data is 100% secure. It will always be a constant battle between hackers, scammers and companies that hold our personal information.

Sometimes it seems that the bad guys are winning – but if you start to implement the precautions on this list, you will go a long way towards keeping your information out of the hands of those bad guys.

Start Today!