How to Avoid Becoming a Victim of Cybercrime

Tony Hanson

aehanson@swbell.net

http://rayson.us/aehanson

Hackers and scammers are actively trying to gain access to your computer and to your personal and financial information. This presentation will help you understand what they are doing, how they are doing it and provide you with steps you can take to minimize the possibility that you will become a victim.

How Scammers Attack

Phone Calls

They utilize Social Engineering techniques and pretend to be somebody or something they are not with the goal of tricking you into revealing private or sensitive information. Typical scams include posing as your local police department, government officials, financial institution or a technical support organization. Blackmail over alleged extramarital affairs or pornography viewing is becoming increasingly common. Technology allows them to display false information on your CallerID device.

They will try to get information from you and may demand immediate payment to avoid arrest, seized bank accounts or public humiliation.

Be very careful about the information you provide to callers. Do not disclose personal or private information. If you suspect the issue/problem is legitimate, hang up and call back using legitimate, independently obtained phone numbers.

The Internet

Avoid obvious scams such as bogus business offers, useless health care offers, offers for discount software and schemes to help people transfer money.

Information from Pop-up ads should not be trusted.

- Never call the phone numbers provided
- Never click on links contained in the pop-up

If you are confronted with a persistent pop-up that you cannot delete, try:

- Closing your browser
- Closing your browser and re-booting your system

HTTPS

HTTPS (HTTP Secure) in an enhancement to the Hypertext Transfer Protocol that is a fundamental component of the internet. Using it insures that malicious parties will not be able to intercept and monitor links you establish to websites that support it. When available, you should take advantage of being able to establish your sessions using HTTPS.

- Google's Chrome browser will tell you that http links are "Not Secure". This is not necessarily true…
- http links are not as secure as they could be: the owner of the website just hasn't paid to upgrade their interface to the more secure https.

Malware

Short for Malicious Software – an umbrella term used to describe software that has malicious intent. It is frequently downloaded when clicking on links found on pop-ups, Spam and Phishing attempts. Malware can steal your contact information, scan your email and files for banking and financial information, destroy files, lock up your PC and demand a ransom, perform surreptitious monitoring of your activities and surreptitiously use storage and processing from your computer for a variety of illicit or illegal activities.

EMail

Spam is email sent to a large number of recipients (typically when somebody's computer is infected with Malware). It typically has an unusual topic, is from an unexpected source and has attached files or embedded links.

Phishing is email or web pages designed to look like they are from a legitimate business or other source. They can be identified by poor grammar, formatting errors and links that do not appear to be going to a site associated with the source. The links frequently take you to websites that appear legitimate.

EMail Rules to Live By:

- Be alert for unusual content of mail received from unexpected or unknown sources
- Be very suspicious of attached filed
- Do not click on embedded links

Smishing – Phishing attempts sent to your Cell Phone as a text message (sent via the SMS channel: SMS Phishing)

Public Wi-Fi

Wi-Fi available in public places, such as libraries, airports, restaurants, hotels or at conferences. It is a shared resource: with the right technology others may be able to see what you are typing. You may also be connecting to a scammers fake network that is designed to look like your hotel or conference network.

When you are connected to a public Wi-Fi network you should assume that your information may be compromised.

If you are in a public place and need to disclose personal or private information:

- Use your cell phone with the Wi-Fi disabled
- Connect your tablet or computer to your cell phones using its Hotspot capabilities

Home Wi-Fi

Take steps to ensure that your home Wi-Fi network is secure. This is becoming increasingly important as wireless intelligent devices (such as thermostats, door bells and intelligent speakers) are emerging.

- Use a strong, complex password to secure wireless access
- Make sure your network is using the WPA2 security protocol (not the weaker WEP)
- Give your Wi-Fi network a nebulous name (Grandmas Network, FBI Sting Network) rather that using a name that discloses your service provider or device type
- Remember that your router is a computer too. It has firmware that should be updated periodically.
- It is also a good idea to replace your router every 3 – 4 years. This insures that you have the latest capabilities and most up to date defenses working for you.

Indirect/3rd Party Attacks

Information about you (and many others) is obtained when hackers penetrate government or large corporate systems, disclosing your name, address, identity information, financial information as well as your UserID and Password.

Having this information makes it easier to scam you using Social Engineering techniques.

If you use the same UserID and Password on multiple systems scammers will be able to access other accounts you have.

If you use weak/common passwords it may be possible for scammers to hack into other accounts you have.

Has Your Email Account Been Exposed?

Enter your email address at this site to see if it has been compromised by hackers:

https://haveibeenpwned.com/

Protecting Yourself

Passwords

Passwords are ubiquitous… You need them to access just about anything. But managing all those passwords is hard work, and the temptation to cut corners is strong. Unfortunately, the day when you could get by with using the same password on multiple accounts is long past.

Let's start my looking at the characteristics of a 'good' password:

- It should consist of at least 10 characters (more characters are more secure)
- It should be complex, which means it should be a combination of letters (UPPER and lower case), numbers and special characters (such as $, _ or !)
- If should NOT contain obvious information (such as your Social Security Number, Phone Number, Address, etc…)
- It should NOT contain any word that can be found in a dictionary
- It should be unique (only used on one account)
- It should be one that you have never used before
- You need to be able remember it

Sounds challenging, doesn't it? Here is one approach that may work for you.

- Start with a 'base' password. This should consist of a combination of letters and numbers that is easy to remember.
- Precede it, or follow it (or both) with a special character or two.
- Precede (of follow) that with a character string that is based on the site it will be used on.

An example may help make this clear.

- Your 'base' can be the first (lower case) letter of each word of a specific phrase that is memorable to you, such as "*The Beatings Will Continue Until Morale Improve*s" – **tbwcumi**
- I entered the workforce when I graduated from college in 1978, so I could append '78', making base **tbwcumi78**
- That was when I started making good money, so I will add a dollar sign: **$tbwcumi78**
    - Oddly enough, some sites will not allow you to use a special character, so just drop it for those sites.
- Use this base to create a password for each site by adding three upper case characters based on the site:
    - Facebook: **FBK$tbwcumi78**
    - Twitter: **TWI$tbwcumi78**

You may also want to utilize stronger (longer) passwords for some of your more sensitive accounts (banking, financial, etc.). Maybe throw in another special character (**CHB$tbwcumi78#**).

When it is time to change passwords (something you should do *at least* once a year), select a new phrase, create a new base and select a different special character ("*Nobody Likes A Sore Loser*" becomes "**!nblasl**") and you will be able to create new passwords that any site should accept.

Why is all this necessary?

- **Complexity** – Creating complex passwords and avoiding the use of 'real' words makes it harder for hackers to compromise your accounts using brute force (i.e. guessing) attacks. Hackers also often try passwords frequently used by others (obtained by hacking into government or corporate systems and obtaining lists of passwords). Using passwords that have not been used by anybody else minimizes your risk.

- **Uniqueness** – Once a hacker gains access to somebody's account, they frequently try that password on other accounts owned by that victim. If you do not recycle passwords on other accounts you shut down this avenue of exploitation.
- **Changing them often** – Unfortunately, some large and widespread security breaches go undetected or unannounced. For example, in late 2017 Yahoo belatedly announced that information for every Yahoo account had been disclosed – in August 2013. For four (4!) years, Yahoo users were completely unaware that their passwords were known to the hacker community. Changing you passwords on a regular basis and following my other recommendations minimizes your exposure to risks like this.

Password Managers

As you probably are well aware by now, remembering all of your passwords (especially if they are all unique and follow the complexity requirements outlined above) is just about impossible. No doubt you have them recorded somewhere… in a file on your PC, recorded in notebook, or on a piece of paper tucked somewhere in your wallet. But there is a better way.

You need to use a Password Manager, such as LastPass, Dashlane, True Key or one of the many other available products.

Many people refuse to even consider this step for a variety of reasons, most of which revolve around the "but what if my password manager account is hacked?" question.

That would be bad. Very bad. And very unlikely, if you:

- Choose a well-designed Password Manager that has adequate security measures, and
- Be extra paranoid about your login credentials (long, complex, never before used passwords)

To all you nay-sayers I can only say "I feel your angst" … I used to be one of you. But I bit the bullet and can honestly say that using a password manager was one of the best things I have ever done to improve my personal security. Here are a few reasons why:

- I can access my information anywhere, any time.
- Because I know I can always get to it no matter where I am, I have been much more willing to actually do all of the things I outlined above.
- It has tools that will alert me to duplicated or weak passwords.
- I have a record of every one of my online accounts. When a security breach occurs, I have one place to go to access all of my accounts and change passwords.
- I am on the board of a non-profit that utilizes a password manager, and I have seen the alerts it provides when an *authorized* user accesses it from a new location or from a new device, so I have a lot of confidence that it will alert me to unauthorized or malicious activity.
- I have made arrangements for my wife and my executor to be able to access my information when I die, and that gives me a lot of comfort.

Sure, there is a risk, but whatever you are using has risks too. I figure that the people running these services have a lot of incentive to work very hard to be sure that their services are as secure as is humanly possible.

2-Step/Two Factor Authentication

Many websites now provide an additional level of authentication when it sees that you are logging in from a new location or from a new device. With 2-step authentication, such login attempts will prompt the site to send a code to your cell phone or email account. If you do not provide that exact code, you will not be allowed to log in.

With this protection in place, unauthorized users will not be able to log into your account even if they have your UserID and Password. As an added bonus, you will be alerted (when you receive the codes) of an attempt to access your account by an unauthorized user. It is definitely something you should enable on every site that supports it.

This capability is offered by many banks and many social media outlets such as Facebook, Google, Twitter and Dropbox.

Security Questions

Many sites prompt you to provide answers to questions that may be used if you forget your password. In many cases, users provide answers that are relatively easy to guess or discover.

Some common questions include:

- What was your first car?
- What was your high school mascot?
- What is your mother’s maiden name?
- Where were you born?

The problem with many of the questions used for this purpose is that the answers are sometimes relatively easy to guess or discover. There are only so many car manufacturers, and many people inadvertently reveal useful personal information on Social Media profile pages.

The thing to keep in mind is that this is one time in life when “honesty is NOT the best policy”. Nobody (besides you) is ever going to know what answers you provide, so why make it easy for the hackers? Make your first car a “a blue bicycle”, your high school mascot “the class president”, your mother’s maiden name “born to be wild” and say you were born “in a manger”.

You can also take your ‘normal’ responses and modify them in some way. For example, instead of saying that your favorite car was a ‘chevy’ you could use these as answers instead:

- ChevyChevy (Repeated)
- yvehc (Reversed)
- Chevyyvehc (Repeated & Reversed)

The goal is to come up with some easy-to-remember scheme you can use to provide uncommon, unexpected, unpredictable answers to these questions. Doing this will make it much less likely that somebody will be able to guess your answers.

Keep Software Current

Keeping your software up to date is an important part of protecting yourself from cyber-attacks. Software providers and equipment manufacturers are constantly providing updates that include the latest security patches designed to protect you and your information.

You should make sure that your operating system, applications and firmware for all of your hardware devices are being updated newer versions become available.

Patches: These are usually small updates provided to address security issues and other critical issues. They are generally provided at no cost and should be loaded as soon as they become available.

New Versions: These are usually major upgrades (for example: Windows 10) that generally include significant security enhancements. There may be a cost associated with the upgrade.

- Free upgrades should be loaded as they become available
- You should always try to remain within one release of the most current version.

Don’t overlook your hardware… Firmware upgrades are frequently distributed for Personal computers, routers and other peripheral devices.

Home Phone

There are not may things you can do to cut down on robo and nuisance calls, but these steps will help:

- Register your number with the National Do Not Call
  Register: **https://www.donotcall.gov/register/reg.aspx**
- Use Caller ID: Only answer calls from people or businesses you recognize
- Let suspicious/unknown/out of ares calls go to voicemail

Mobile Phones

If you do not recognize the number calling you it is best to not answer the call. Answering a telemarketer’s call will usually result in a lot of repeat calls.

Your cellular phone offers more privacy options that a conventional landline that you use to manage your incoming calls.

- Register your number with the National Do Not Call
  Register: **https://www.donotcall.gov/register/reg.aspx**
- **Contact List** – Keep this up to date with information about people you frequently interact with. Your phone will recognize phone numbers and display accurate information about these people when they call you.
  - Only answer calls from people or businesses you recognize
  - Block numbers that call frequently and never leave a message
- Take advantage of provider provided privacy tools:
  - **AT&T Customers** – Download and use the free Call Protect app to enable automatic fraud blocking and suspected Spam warnings.
  - **T-Mobile** – Get **ScamID** for free, can enable **ScamBlock** at no cost too.

  - **Verizon Customers** – Call Filter will be available at no cost beginning in May 2019.
- Load and use Apps to interact with businesses. They provide good features and are much more secure than using their browser interface
- Only download apps from legitimate sources:
  - Apple Store
  - Google Play Store
- Keep your software (including your apps) up to date.
- Lock your device with a password (and a bio-metric scan, if supported by your device). Longer/complicated passwords will provide more protection.
- Make the inactivity time required to lock your phone short (no longer than 60 seconds)
- Make sure that your phone is being backed up on a regular basis
- Enable your phone's flavor of the "Find My Phone" feature so you can locate (and lock or erase it) if you lose it.

Windows User? Use Anti-Virus Software

Anti-Virus software provides an additional layer of defense when you are dealing with email, websites and flash drives. This is vital for Windows users.

Microsoft 10 comes with Windows Firewall and Windows Defender. These are both very capable products that you should be using. However, adding a 3rd party Anti-Malware/Anti-Virus package adds a vital additional level of protection.

Google "Anti-Virus Software" to obtain information about currently available software. This is something you should review every year of so… If your current product is no longer one of the top-rated solutions consider changing to a more effective product.

What about Apple Products?

Apple does a good job of keeping their operating environments secure. As long as you only download software from their App store you probably do not need Anti-Virus or Anti-Malware software – according to this article: '**Do Macs need antivirus software**?'

Also see '*All about Mac antivirus*' – **https://www.malwarebytes.com/mac-antivirus/?utm_source=double-opt-in&utm_medium=email-internal-b2c&utm_campaign=EM-B2C-2018-May-newsletter&utm_content=macbookT**

What about Android based Mobile Phones?

As with Apple products, Anti-Virus and Anti-Malware software does not appear to be a necessity. Google reportedly also does a good job of keeping their platforms and apps distributed through Google Play secure, according to this 22 December 2017 article: '**Do you need antivirus on Android?**'. You may also be interested in the 24 August, 2017 article titled '**Why you don't need antivirus on Android (in most cases)**'.

Freeze Your Credit Reports

Freezing your credit reports makes it difficult for anybody to fraudulently open a credit account using your identity. There are three or four (depending on who you believe) credit reporting companies:

- Equifax
- Experian
- TransUnion
- Innovis

You can contact each company and place a freeze on your credit account. This means nobody should be able obtain your credit information and create a new account in your name. This is good from a privacy and security perspective, but it may present you with some real-world hassles (and cost you some money too).

You must contact each company separately and follow their procedures (and pay their fee) required to put the freeze in place. Then, if you ever have a legitimate need for somebody to obtain your credit report (to, for example, obtain a new credit card or take out a loan), you will need to contact the appropriate company and follow their procedures to unlock your account.

You should also be aware the big three companies (Equifax, Experian and TransUnion) are required by Federal Law to provide you with a copy of your own credit report once each year, if you request it. There is no charge for this report. However, if you want the report you will have to go through the unlock/locking process (paying more fees along the way) to get it.

If you are interested in keeping an eye on your credit reports (with or without freezing your accounts) you can request a report from each a different company every 4 months. That way you may spot unusual activity more quickly.

The AnnualCreditReport.com website (**https://www.annualcreditreport.com/index.action**) is a good source of additional information on Credit Reports.

Backups

Backups are your ultimate defense against Ransom Ware and catastrophic damage to your computer. You should be backing your data up three different ways.

Windows and Mac systems have native backup utilities that you should be using to create regular, scheduled backups. However, since these are usually created on disk drives that are in (or near) you computer you should also be creating at least two other backups.

Cloud based backup services (such as Backblaze, Carbonite, CrashPlan, Mozy and others) provide a low cost and secure way to create an off-site backup of your data. Best of all, they are automatic: all you need to do is sign up for the service, install the software and let it do its thing.

Your third backup should be made on a USB attached disk drive. High capacity devices are now available at a very reasonable cost, especially if you catch one on sale. For maximum protection, only connect the drive to your computer when you are actually copying files (once a month is probably sufficient for most people). The rest of the time disconnect the drive and store it in another room.

Your USB backup can serve as your ultimate defense against a Ransomware attack. If your system ever should be locked up you can start from scratch and not lose more than a month's worth of changes. That may be a better alternative than paying hundreds of dollars to unlock you hijacked PC.

Files Containing Sensitive Information

Take care of files that contain sensitive information.

- Delete the files if they are no longer needed.
- Encrypt files the you do keep. See '*The Best Encryption Software of 2018*' (**https://www.pcmag.com/article/347066/the-best-encryption-software-of-2016** – PC Magazine – December 12, 2017) for reviews of encryption software.

Delete Messages with Sensitive Information

Don't leave sensitive information where malware can find it!

- If you receive a message that contains sensitive information, delete it as soon as possible
- If you send a message that contains sensitive information:
    - Ask the recipient to delete it as soon as possible
    - Delete the copy the message that your email package saves in your Sent Message Folder