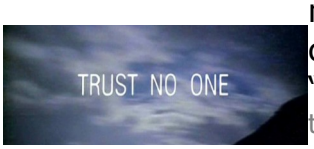
Cyber Security

An Introduction to Computer Security, by George Lazarides.

This document, and this presentation, are not the know-all and end-all for security, this is just a beginning for you, a "Cyber Security 101," so to speak.

In modern times Cyber Security may be one of the most important things to know about and understand, at least on a basic level. You can't think of security as a "one-and-done" deal, security is something you need to cultivate and nurture. One of the sayings that is popular regarding computer/internet security is:



"Trust No One" (**TNO**) [originally made popular in *The X-Files*, applied to computer security by Steve Gibson, whom has been doing the "*Security Now!*" podcast since 2005 https://twit.tv/shows/security-now].

Some reasons to take Cyber Security seriously:

- Identity Theft
- Crypto-Ransomware
- Data Theft
- Money Theft
- National Security
- Network Bandwidth Theft (Distributed Denial of Service [DDoS], Spam)
- Computer Processing (and electrical) Power (Cryptocurrency miners)
- Invasion of Privacy (Emails, Cameras, Microphones)

The City's Information Technology (**IT**) Department takes the security of its computers and networks seriously, and we do what we can to secure everything we have domain over.

Something to remember is that no one-thing that you do to protect yourself from security threats will be 100% effective, so I like to recommend a multi-layered approach to securing yourself online.

Cyber Security is …

- A balance of security and convenience. The more inconvenient security is, the more likely that some users may weaken areas of security that they have control over (such as passwords).
- A game of cat-and-mouse, as the good guys patch security holes, bad guys find more security holes.

So those in the IT industry always need to make good security as easy as they can for the user, and all of us need stay vigilant in our fight to stay secure.

Patches ...

Most software patches come out for security reasons, **keep your Operating System (OS) and Application Software patches up-to-date**. Here at work we might not have the ability to control the application of patches, so just keep the things patched that you can patch.

Antivirus ...

Most people should run an antivirus on their computers, *Microsoft* has a good free one called **Windows Defender** that many security conscious people use. We use the **ESET** antivirus here on the City's computers.

Like "patching" you need to make sure that your antivirus stays up-to-date so that it can block everything it knows about.

But you need to realize that antivirus programs will not stop every threat to your computer, they can only stop the ones that they know about. What they don't know about are called "Zero Day Attacks" or "Zero Day Threats," which may be out in the wild (infecting computers) for a long time before they are discovered.

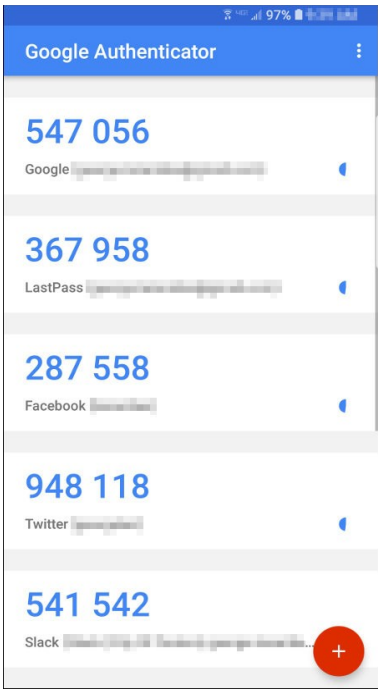
Passwords ...

As users, our primary line of defense (that we have direct control over) against bad guys is our passwords. Don't take it for granted that just any password will keep the bad guys out, make a good password.

Password Tips:

- Longer is stronger, add a pattern of characters to lengthen it (ex. '`MyStr0ngP@ssword-=-=-=-=-=-`'), you can use https://www.grc.com/haystack.htm to test basic password strength.
- Don't use simple words, "Dictionary Attacks" can crack a password in a matter of seconds.
- "Rainbow Tables" keep track of words and phrases that have been "seen" by hackers, Rainbow Tables can also defeat passwords in seconds.
- Do not re-use passwords on multiple sites, especially if the sites are "High Value" sites such as banking, shopping, email, social, or work sites.
- Use a good password manager to remember all of your different passwords for you, such as **LastPass** (lastpass.com), or **Bitwarden** (bitwarden.com).
- Have your password manager generate long, random passwords for you.

Two Factor Authentication (2FA) …



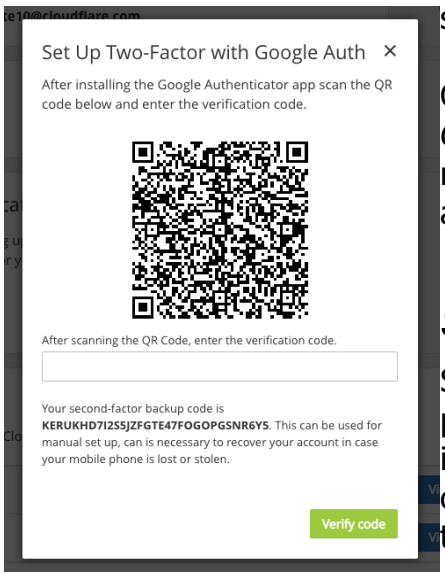
Different factors of authentication are:

- Something you know
  username and password
- Something you have
  phone (SMS Messages), time-based security codes (Google Authenticator), single use passwords, key fob, USB dongle (YubiKey), computer (cookies)
- Something you are
  bio-metrics – fingerprint, face, eyes, hands

2FA requires you to not only enter you user name and password (**something you know**), but it will also ask for a second factor of authentication (**something you have**, or **something you are**).

If a site gives you the ability to use a second factor of authentication, then you should enable it. You also need to be aware that 2FA puts a lot more of the burden of security on you, in that if you lose your "something you have" you may be up-a-creek.

So if you have 2FA attached to your mobile phone number, don't just change your phone number without considering what online accounts you will have to change so that you do not lose the ability to log into them.



One tip is to print out the QR Codes as you add them to *Google Authenticator* so that if you change devices you can re-scan the QR Codes that you printed out and still have access to the accounts they are associated with.

Safe Keeping …

Some people say that you should not print or write any of your security information. I say that you can print or write them, as long as you keep them safe:

- If you print or write a password then **keep it where you keep your credit cards** (you keep those safe, right?).
- If you print a QR Code (*Snipping Tool* and *Snip & Sketch* work great for this), write what it's for on the printout, then **keep it where you keep you important documents at home** (keep it in a "Document Box," a **Fire Safe** would be perfect).

Browser Security …

There are countless ways to secure your internet browser, each of which have varying degrees of effectiveness.

One add-on you may want to look into is "**µBlock Origin**," it is a browser add-on for all of the major browsers. It blocks most 3rd party scripts (programs that run in your browser) from running on your system. It is worth noting that these add-ons can "break" some sites, so they might not be for you.

Browser Notifications …

Another avenue that some bad guys use is browser Notifications.

You may have noticed some of the web sites that you visit have the browser show you a popup that asks if you would like to enable Notifications on your browser for their web site. A good rule of thumb is to **always deny** them that access to your browser.

Browser Notifications are push notifications that allow them to send notifications to your browser at any time (even when you are not on their web site). Many of the web sites use a third party service for their browser notifications, so even if the website itself is trustworthy, the service that they use may not be trustworthy. Those third party services are also targets of hackers because if they can compromise their service, then the bad guys can send out messages to many people at once. If a user clicks through a message, they could instantly have their computer compromised, also making their network more vulnerable.

In your browser settings you can review weather you have **Allowed** or **Blocked** any web sites, you are also able to change the setting on each site. You can also disable the browser's ability to show you those requests, thus effectively blocking all future sites' Notifications.

Your Email, and Social Accounts …

This is the most important aspect of computer and internet security that you have the most control over, so this is where you have to be the most diligent and engaged with your security. Initially Operating Systems (**OS**) used to be the most vulnerable part of the computer/internet ecosystem. Over the last 20+ years computer OSes have gotten more secure and over the last 10+ years applications have also been getting more secure, so hackers have been changing their targets to be able to get into computers.

So what is the most vulnerable target that hackers can get to?

YOU! 

Yes, most computer users are the softest targets that hackers have access to. So this is why we (as computer users) need to train ourselves to be alert to the many machinations that the hackers use … or even *might* use.

These hackers even come at us through our social accounts (Facebook, Twitter, Instagram, etc.) and try to "friend" you making you think they are a current friend that may have changed accounts. If someone tries to "friend" you, do the extra footwork to determine if they are who they say they are **BEFORE** you accept them. They may actually be a stranger trying to get you to send them money, gift cards, etc.

Gone Phishing!

Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social engineering schemes use spoofed e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. Technical subterfuge schemes plant malware onto PCs to steal credentials directly, often using Trojan keystroke logger spyware. **Pharming** malware misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or DNS poisoning.

The number, and sophistication, of phishing scams sent over the internet is continuing to increase. We here at the City have seen an increase of Spear Phishing (see below) attacks. While online banking and shopping is very safe, as a general rule you should be careful about giving out your personal financial information over the Internet. Make sure the web site your browser is on is the web site you expected it to be on before you enter your personal information.

Spear Phishing, targeted, attacks are not only personalized (they seem to know you, and address you by name), but also seem to come from authoritative or trusted sources. Spear Phishing attacks are often perpetrated by state level actors (Russia, China, North Korea, etc.) to get into sensitive networks or acquire sensitive information, and by criminals trying to get ransomware installed on computers in your network.

***IMPORTANT*: Don't Click It ...**

If you weren't expecting a particular email that is asking you to click a link; look at a file; or install software, or if you were on a web site and a message tells you, "You have a virus, click here to remove it!" **DON'T DO IT!** At this point your "*Spider-Sense*" should be tingling. Report anything you are suspicious about to the IT Department.

"Never install anything you didn't go looking for."
- Brian Krebs (computer security expert)

As explained by *Steve Gibson (computer security expert)*:
"If something offers you software, just say, 'No.'
Unless you initiated the search (for the software), don't install it, period."

USB Drop Attacks...

You are walking in to work from your car, and oh, look! There is a USB Flash Drive on the ground in the parking lot!

WOW! It must be your lucky day!

Or not.

DO **NOT** PLUG THAT USB DRIVE INTO YOUR COMPUTER!

This is another way for hackers to get into your network: they have **you** bypass most of the security that is in place, and have **you** put an infected USB drive directly into your computer. Most computers will automatically execute "Auto Run" programs that are on a USB drive, and in this example it will automatically infect your computer, with little (or no) input from you.

This type of attack is most often the work of adversarial state level actors (such as Russia, China, and North Korea), they are very motivated to penetrate into as much of our country's government, infrastructure, and financial institutions as they can. This is part of the new Cyber Warfare that is being waged every day now.

Don't do the hackers work for them! They may need someone like you to get them past all of the network and computer security that we have in place.

If you do find a USB Drive on the ground, whether outside or inside, take it to the IT Department and let them examine it, they may even turn it over to the FBI.

Viruses ...

As a user on your computer, if it is possible you should not run as an Administrative User, but rather a Limited (Standard) User. This helps prevent viruses from getting a foot hold in your computer.

If the OS asks you if it's OK to install some software, **STOP and think** for a moment to see if you **really** trust the software that's being installed.

If a virus does make it past all other security measures, **you** may be the last and best line of defense. Be smart, be strong, be vigilant.

Layers of Security...

Since there isn't one single "silver bullet" that can protect you from all of the attacks that come at us on our computers and networks, you need to cover yourself in layers of security, here are some layers to consider:

- Firewall
  (on your computer and network [NAT router])
- Antivirus
- Patching (OS and applications)
- Good Passwords
- Two Factor Authentication (2FA)
- Script Blocking
- Your "Spider-Sense" that stops you from clicking bad links or installing bad software
- Don't visit shady sites or click links in unexpected emails

Attacks Happen ...

I've been keeping up a web page at https://app.cantonohio.gov/it/?pg=756 since 2013 to be transparent with the public and our users about security incidents we have run into. Feel free to peruse that page to see some real-life examples that affected the City of Canton.

Transparency in regards to security, and especially lapses in security, helps to foster trust. This transparency is something that we should expect from the organizations that we have contact with. If a company, or organization, or individual, says that there are "no problems, everything's fine," or that they have never had to deal with security issues then they are either lying, or they are clueless as to what is going on in their network.

If an organization lies about, or hides, security incidents from their users and the public, then they will rightfully lose most (if not all) of the trust that they once enjoyed. That trust will not be easy to regain, if it can be regained at all. The best practice is to be open and transparent about security from the beginning.

Got hit by Ransomware?

Try https://www.nomoreransom.org before you pay.

Ransomware Targeting Infrastructure, Schools, Cities, and States...

In recent years the bad guys that are pushing out ransomware have been realizing that organizations such as airports, cities, and states, have much deeper pockets (have more money) than an individual.

Since 2018 Ransomware has been hitting many cities in most states, notably Baltimore ($10,000,000 ransom), several cities in Florida, and over 30 cities in Texas (22 of them were victims in a simultaneous coordinated attack). It has also been hitting state level governments in the United States, the highest profile incident was in Georgia. Each of these incidents can come with a ransom demand in the 6 figure range (or higher), so you can see there is definitely an incentive for the bad guys to keep doing what they are doing.

"I repeat the saying I've heard came from inside the NSA:
'Attacks always get better; they never get worse.'"
- *Bruce Schneier (computer security expert)*

On a more local level

Cleveland Hopkins International Airport was hit with ransomware.

Akron was hit by ransomware and had to pay the ransom.

Here at the City of Canton a significant department was hit with ransomware because a user opened an email attachment from a Spear Phishing email, but we had good backups to recover from, they only lost a day of input. Unfortunately somehow the network got re-infected, causing us to recover from the same backups again.

The attack vector on each of these incidents was an email Spear Phishing attack. These attackers could send out 1,000,000 emails, and 999,999 might be ignored or deleted. If just one person clicks on the file attachment and allows it to run, the whole organization can be affected. Ransomware could run rampant on the computers in the network, costing the organization not only money and time, but possibly their reputation.

All because of one person.

DON'T BE THAT "ONE PERSON" !!!