Browsing the Web Safely

QUESTIONS? EMAIL US: INFO@HAMDENLIBRARY.ORG

PDF AVAILABLE AT: HAMDENLIBRARY.ORG/COMPUTERLAB

Topics

Browsing: HTTPS

Browsing: Secured and Unsecured Wi-Fi Connections

Browsing: Downloading and Viewing Files

Browsing: Website Red Flags

Browsing: Pop-Ups

Online Accounts: Passwords

Online Accounts: 2-Step-Verification

General: Backup Data to defeat Ransomware, crashes and other bugs.

General: Windows Defender vs 3rd Party Anti-Virus General: Firewall

General: VPNs

What is HTTPS?

Stands for Hypertext Transfer Protocol Secure (a secure version of HTTP)

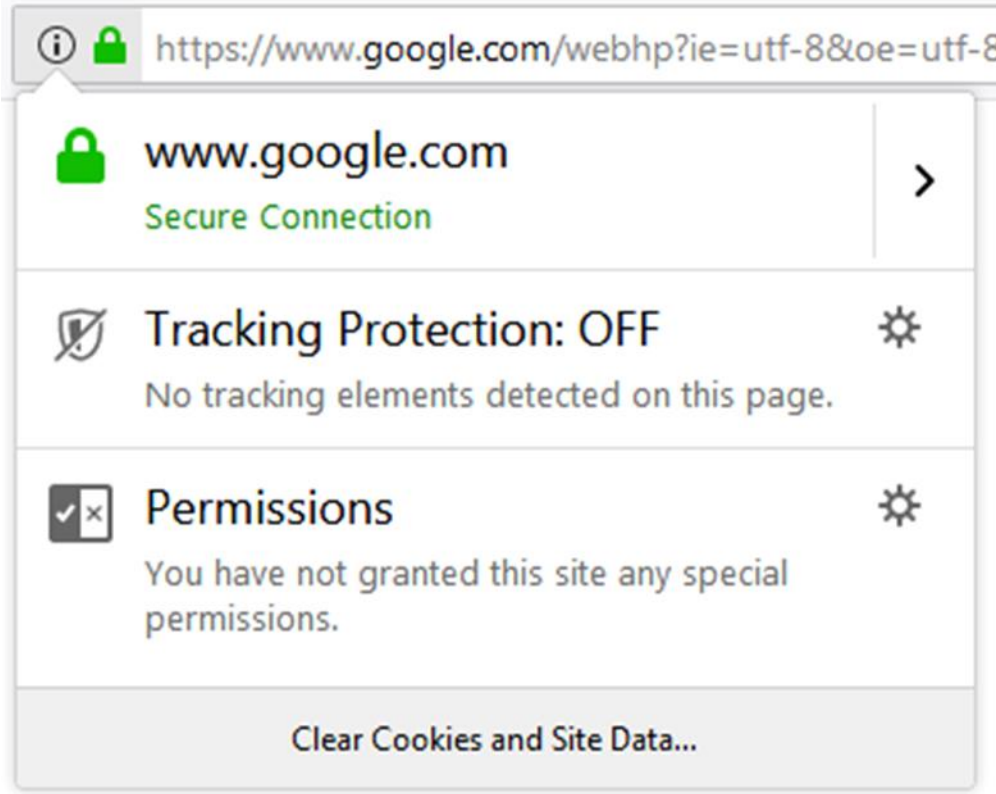
HTTP is the foundation of data communication on the World Wide Web.

HTTP works using a client/server model. One computer, the client, requests a website/resource from another computer, the server, which then sends the appropriate information back to the client.

These requests, which may contain personally identifiable information (including passwords), often pass through many other computers between the client and the server.

HTTPS prevents others from viewing information travelling between you and the website by encrypting the data while it is being transferred over the internet. Others can still see the sites that you are visiting but won't be able to see anything else.

https://www.eff.org/pages/tor-and-https



HTTPS://continued

Additionally, some websites also use HTTPS for logging in but then default back to unencrypted HTTP connections.

You can use Browser extensions/plugins like HTTPS Everywhere in order to force websites to use the HTTPS connection automatically.

https://www.eff.org/https-everywhere to find out more about HTTPS Everywhere

HTTPS is not a guarantee that a site is legitimate. Cyber criminals can buy security certificates themselves.

Wi-Fi: Secured vs. Unsecured

Unsecured Wi-Fi:

- If the network does not require a password, its probably not secure
- Anyone can monitor and steal the data being sent over the network (particularly if connected to an unencrypted site)
- If you must use an unencrypted Wi-Fi network, make sure the site you are using is HTTPS encrypted
- Make sure the entire site is encrypted, not just the login page
- If you regularly use unsecured Wi-Fi networks, consider using a Virtual Private Network service to encrypt your traffic

Secured Wi-Fi

- Will require a password
- Encrypts data moving between itself and the internet
- Even on a secured public network it is risky to do anything that requires financial information (bank websites, online shopping)

https://www.consumer.ftc.gov/articles/0014-tips-using-public-wi-fi-networks

Wi-Fi: at Home

Change your router’s default name and password to something unique and secure.

Change the password once in a while.

Change the routers administrator account name and password as well.

Make sure your router’s software is up to date by checking with the manufacturer or your internet service provider.

Disable any remote management features.

Make sure your router has WPA2 encryption capability (Wired Protected Access 2). If it doesn’t, see if there is a software security update for your router to get to WPA2.

Downloading and Viewing Files

Many common viruses and malware programs are often installed on your system when you download and open an infected file.

These files can take the form of email attachments, software programs downloaded from websites or pop-up ads, or even files on physical devices like USB drives.

Emails:

- Read the email carefully and look for anything unusual.
- Don’t download or open attachments that you are not expecting.
- If you get an attachment you weren’t expecting from someone you know, contact the person and confirm that they actually sent the file if you are unsure.

Downloading files or software from the internet:

- Only download from places you trust.
- If you are unsure about a website, do some research and look for information or reviews about the site/product from another source, if you are still unsure do not download.
- Never download anything from a pop-up, especially if it claims that “Your PC is infected!” or something similar
- If possible, use a non-Administrator account for day-to-day browsing as these types of accounts are not permitted to install new software on the computer.

Website Red Flags

Not HTTPS: especially for financial or personal information, not having HTTPS is a big giveaway

Unbelievable prices/sounds too good to be true,

Bad Spelling/Grammar or odd word phrasing

Having a spoofed URL address

- A spoof URL is a Website address that is attempting to look like the address of a legitimate site.
- https://myaccount.google.com is a real address
- http://myaccount.go0gle.com is a fake address (misspelled)
- http://google.myaccount.com/ is a fake address (doesn't end in google.com/)
- Other spoofs use non-Latin letters in order to make a URL appear identical to a companies website, https://www.xn--80ak6aa92e.com/ for example appears as https://www.apple.com/ in Firefox.*

*To make Firefox display the right URL, go to **about:config** in the address bar, agree to the warning, search for **Punycode,** find **network.IDN_show_punycode** and change it to **True**

Pop-Ups

Pop-ups are annoying little windows or images that appear on the screen in front of what you are looking at usually with advertisements

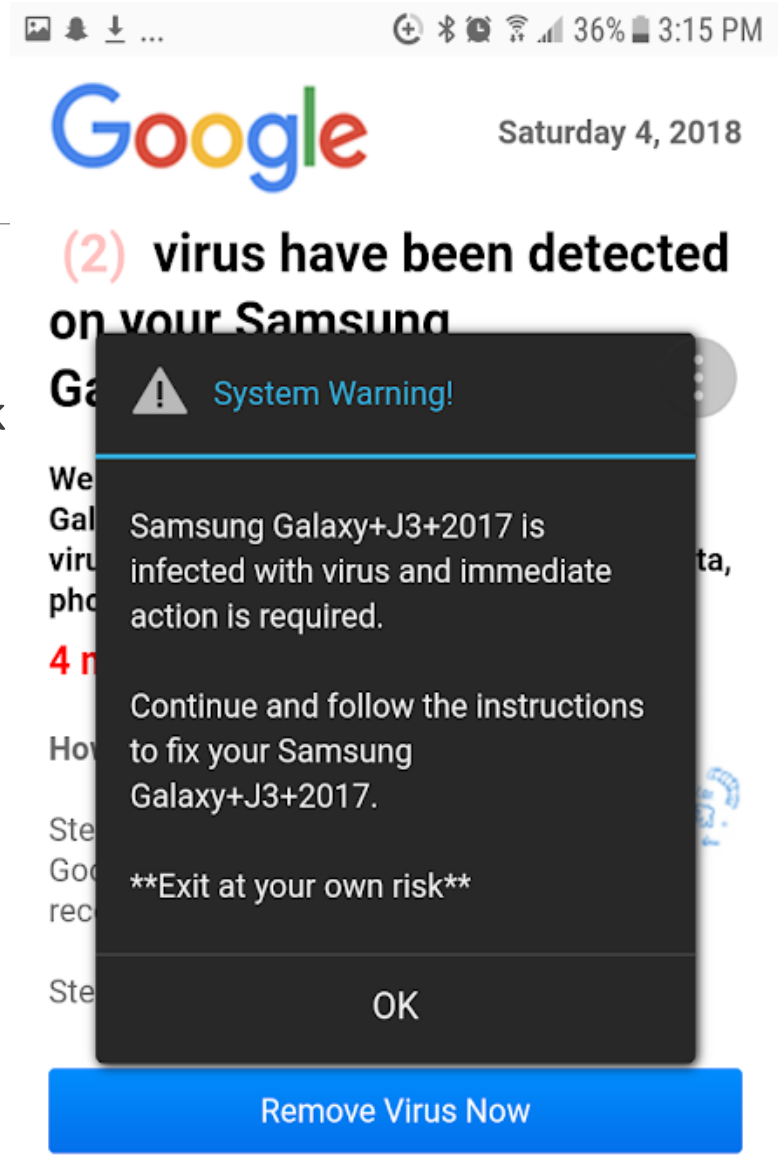
Malware can often hide in ads like this and often try to get you to click on a link or anywhere on the popup. Some may even try to prevent you from closing it.

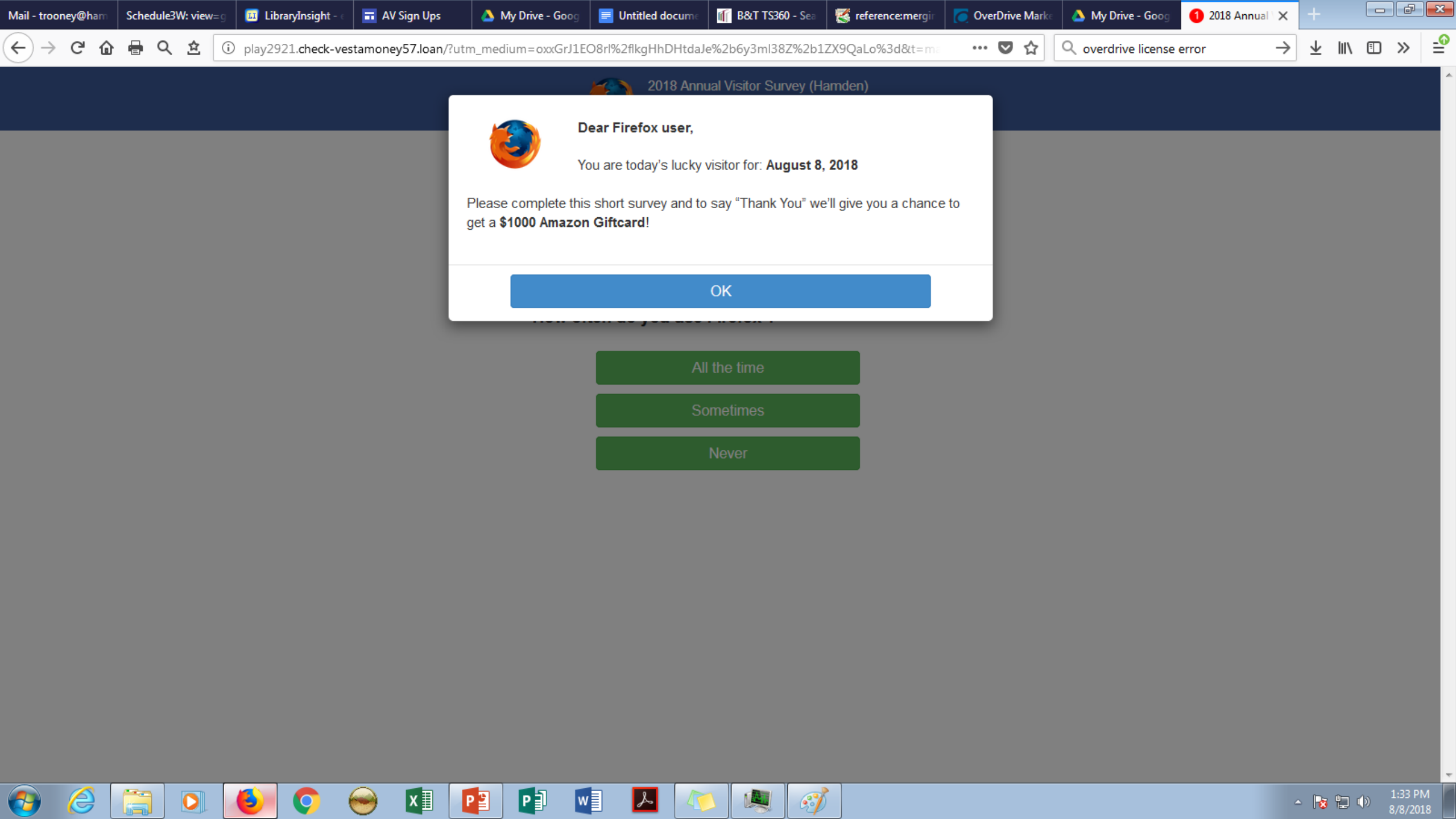
Popular scams involving saying you won some sort of contest or that your device is infected, with the pop up pretending to be either the hacker or a security company

These popups try to frighten you with trivial information (your location or device type/name)

They also try to make you act before thinking by implying immediate consequences for inaction

Never click on these pop-ups, exit out of the browser or restart the device if necessary




Mail - trooney@ham
Schedule3W: view=g
LibraryInsight -
AV Sign Ups
My Drive - Goog
Untitled docume
B&T TS360 - Sea
reference:mergir
OverDrive Marke
My Drive - Goog
2018 Annual
play2921.check-vestamoney57.loan/?utm_medium=oxxGrJ1EO8rl%2flkgHhDHtdaJe%2b6y3ml38Z%2b1ZX9QaLo%3d&t=ma
overdrive license error
2018 Annual Visitor Survey (Hamden)
Dear Firefox user,
You are today's lucky visitor for: August 8, 2018
Please complete this short survey and to say "Thank You" we'll give you a chance to get a $1000 Amazon Giftcard!
OK
All the time
Sometimes
Never
1:33 PM
8/8/2018

General Browsing Tips

If you know a website's address, type in the full URL instead of performing a search, which may yield incorrect or even fraudulent results.

Don't stay permanently logged into accounts, logout when you are done.

Stay vigilant, look for website red flags, think twice before downloading, and don't trust things at face value.

Don't act without thinking things through, even if the malware/phishing message is pressuring you to.

If you are not sure about something, hold off, do research and ask others before proceeding.

Try to browse using a non-administrator account to prevent accidently giving a program permission to infect your computer.

Make sure the software on your anti-virus, anti-malware, operating system, browser, and router systems are all up to date with the latest security patches.

Some Tips on Creating Strong Passwords

Never use the same password more than once or for more than one site

Change passwords every so often

Write them down and keep them in a safe place if necessary

How to make a strong password:

- Use upper case and lower case letters
- Use numbers and symbols as well
- The longer the better (shorter passwords are easier to crack)
- Don’t use recognizable words (i.e. **hYd#DH5f%D$j6f3h8$** is a strong password)

Wherever possible, use 2-Step Verification.

Password Managers

Using a password manager helps protect you while also making your life easier. Password managers generate lengthy passwords that are much harder to guess, and they remember them for you. All you have to do is remember one master password. (Of course, you should try to make your master password hard to guess as well.)

Popular password managers include: 1Password , LastPass , Dashlane and Keeper . Check out some of the links below for more information and reviews of these and other password managers.

Further reading:
Consumer Reports - Everything You Need to Know About Password Managers
Wired - Get a Password Manager. No More Excuses.
Wire Cutter - The Best Password Managers

2-Step Verification

Also referred to as 2 Factor Authentication (although they are not technically the same thing)

2 Step Verification allows you to add an extra layer of security to your online accounts.

Whenever someone logs into your account from a new device, a second authorization code is required in addition to the password.

This can be a randomly generated code sent to your phone, a personal security question (i.e. your childhood dog's name), or even a physical key that you plug into the computer.

Why use it?

- If your password is ever compromised, any attacker will require this second method to break in.
- It is highly unlikely that an attacker will be able to gain access to both security methods.

Anti-Virus Software

Anti-virus programs scan your computer's files for infections or malware

They also try to prevent you from accessing or downloading malware as well

There is debate on anti-virus software's effectiveness, but in general it is good to have in order to prevent "drive-by" infections

For windows users, having an anti-virus service on is a good idea

- Windows comes pre-loaded with Windows Defender, Microsoft's anti-virus software
- You can also choose to purchase or download an anti-virus program from another company if you want
- When you install a 3rd party anti-virus service Windows Defender will step back and go dormant so it doesn't conflict with your other antivirus service
- Never have more than one Anti-Virus program running at the same time; they will interfere with one another

Mac users can generally get away without using an anti-virus program, but users can get programs for it if they wish

Firewall

Prevents unauthorized access to your computer from the internet/network.

Windows machines have a firewall enabled by default.

Macs come with a built in firewall but it is disabled by default.

By default the firewall will block all incoming connections to your computer or network that was not requested by your computer.

Outgoing connections are not blocked unless they match a rule.

You can create custom rules to block or allow incoming or outgoing traffic.

Firewalls are important but not all powerful. If you allow malware through the firewall it can send out all the data it wishes, or even create new rules to compromise your firewall.

Back up your data

When your computer gets hit with malware, often a lot of your personal data can be lost, particularly with ransomware

Ransomware: malware that encrypts all the files on your computer and then demands payment for the decryption key. Payment is usually demanded with untraceable means (Bitcoin etc…)

The best way to defeat these sorts of problems is to make backup copies of your data and store it in a different device.

The Rule of Three: a good practice is to have 3 copies of any important information:

- One on your normal computer
- One backup on a physical storage device (USB, External Hard Drive, CD)
- One backup on a cloud storage service (Google Drive, DropBox, BackBlaze)

Keep your backups updated often; the longer you wait between updates, the more data you will lose if you need to start over

The many types of Malware

Ransomware:

- Compromises your files and tires to extort money out of you
- Can either threaten to publish your materials or encrypts your data and demands payment for the decryption key

Virus:

- Attempts to propagate itself by inserting copies into other programs
- Have a range of effects, from ads, to performance drops to destroying data

Worm

- Spread similarly to viruses, different in that they are standalone programs and do not require a host program file
- Often used as a method to deliver other types of malware

Trojan

- Harmful software disguised as a legitimate program
- Tricks users into opening them, does not self replicate
- Create backdoors in systems to allow malicious actors access

Spyware

- Secretly software that monitors your computer usage
- Used to sell advertising info or install Trojans

Bots

- Self-propagating program that connects your computer to a command and control server
- Can make your computer carry out attacks, mine bitcoins or just steal info.

Fakeware:

- Malware masquerading as anti-virus software

Virtual Private Networks

What is it

- A technology that allows you to create a secure connection over the internet to another network
- Originally designed for businesses, so employees could access the company's network from home

What does it do

- Creates a secure "tunnel" between your device and the VPN server through which your internet traffic travels
- Anyone monitoring your internet activity (like your ISP) will only see that you are connected to a VPN service, anywhere else you go will be hidden from them
- Only the VPN service itself will be able to see what sites you visit, but not the content if the site is HTTPS enabled

Why use it

- Encrypts your online activities from even your Internet Service Provider
- Protects your identity
- Get around location blocks and other censorship tools

Resources

HTTPS

- https://www.howtogeek.com/181767/htg-explains-what-is-https-and-why-should-i-care/
- https://www.wired.com/2016/04/hacker-lexicon-what-is-https-encryption/
- https://blog.mozilla.org/internetcitizen/2017/04/21/https-protect/
  https://www.youtube.com/watch?v=d2GmcPYWm5k Into to HTTPS (very long and technical)

Anti-Virus

- https://www.techradar.com/best/best-antivirus
- https://www.windowscentral.com/do-you-need-pc-antivirus
- https://mashable.com/2017/09/18/antivirus-software-free-paid/#VsD9SxqZE5qF
- https://www.tomsguide.com/us/windows-defender-av-test,news-27694.html
- https://www.cnet.com/how-to/i-dont-use-anti-virus-software-am-i-nuts/#comments

Downloading

- https://support.google.com/google-ads/answer/2375413?hl=en
- https://blog.malwarebytes.com/101/2016/08/10-easy-ways-to-prevent-malware-infection/
- https://www.pcworld.com/article/210891/malware.html
- https://support.microsoft.com/en-us/help/129972/how-to-prevent-and-remove-viruses-and-other-malware

Resources

Wifi

- https://gizmodo.com/how-to-keep-your-home-wi-fi-secure-1821008133
- https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network
- https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network
- https://www.consumer.ftc.gov/articles/0014-tips-using-public-wi-fi-networks
- https://lifehacker.com/5576927/how-to-stay-safe-on-public-wi-fi-networks
- https://www.eff.org/deeplinks/2010/06/encrypt-web-https-everywhere-firefox-extension
- https://www.eff.org/pages/tor-and-https
- https://us.norton.com/internetsecurity-wifi-the-dos-and-donts-of-using-public-wi-fi.html

VPNs

- https://lifehacker.com/5935863/five-best-vpn-service-providers
- https://www.pcmag.com/article/364072/do-i-need-a-vpn-at-home
- https://www.pcmag.com/article2/0,2817,2403388,00.asp

Resources

Malware Types

- https://www.dummies.com/computers/pcs/know-the-different-types-of-malware/
- https://www.cisco.com/c/en/us/about/security-center/virus-differences.html
- https://www.umass.edu/it/security/malware-viruses-spyware-adware-other-malicious-software
- https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html

Backups

- https://www.lifewire.com/ways-to-back-up-your-data-2640426
- https://us.norton.com/internetsecurity-how-to-the-importance-of-data-back-up.html
- https://www.backblaze.com/backup-your-computer.html

Firewall

- https://www.howtogeek.com/144269/htg-explains-what-firewalls-actually-do/
- https://www.howtogeek.com/205108/your-mac%E2%80%99s-firewall-is-off-by-default-do-you-need-to-enable-it/
- https://support.apple.com/en-us/HT201642

Resources

2-Step Verification

- https://gizmodo.com/its-time-to-enable-two-step-authentication-on-everythin-1646242605
- https://lifehacker.com/the-difference-between-two-factor-and-two-step-authenti-1787159870

Passwords

- https://lifehacker.com/how-to-create-a-strong-password-1797681069
- https://support.google.com/accounts/answer/32040?hl=en
- https://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/
- https://www.businessinsider.com/hacker-strong-password-2016-4

Red Flags

- https://www.techwalla.com/articles/how-to-recognize-a-fake-url
- https://checkshorturl.com/
- https://www.theguardian.com/technology/2017/apr/19/phishing-url-trick-hackers
- https://9to5mac.com/2017/04/20/how-to-spot-a-phishing-attempt-fake-apple-site/
- https://www.xn--80ak6aa92e.com/ Fake apple website set up by Xudong Zheng, Chinese security researcher. Shows up as Apple.com in Firefox
- https://www.symantec.com/connect/blogs/spoofing-around-urls
- https://news.softpedia.com/news/chrome-firefox-preparing-fixes-for-nasty-phishing-trick-using-punycode-515005.shtml
- https://www.scamwatch.gov.au/types-of-scams/buying-or-selling/online-shopping-scams#warning-signs