



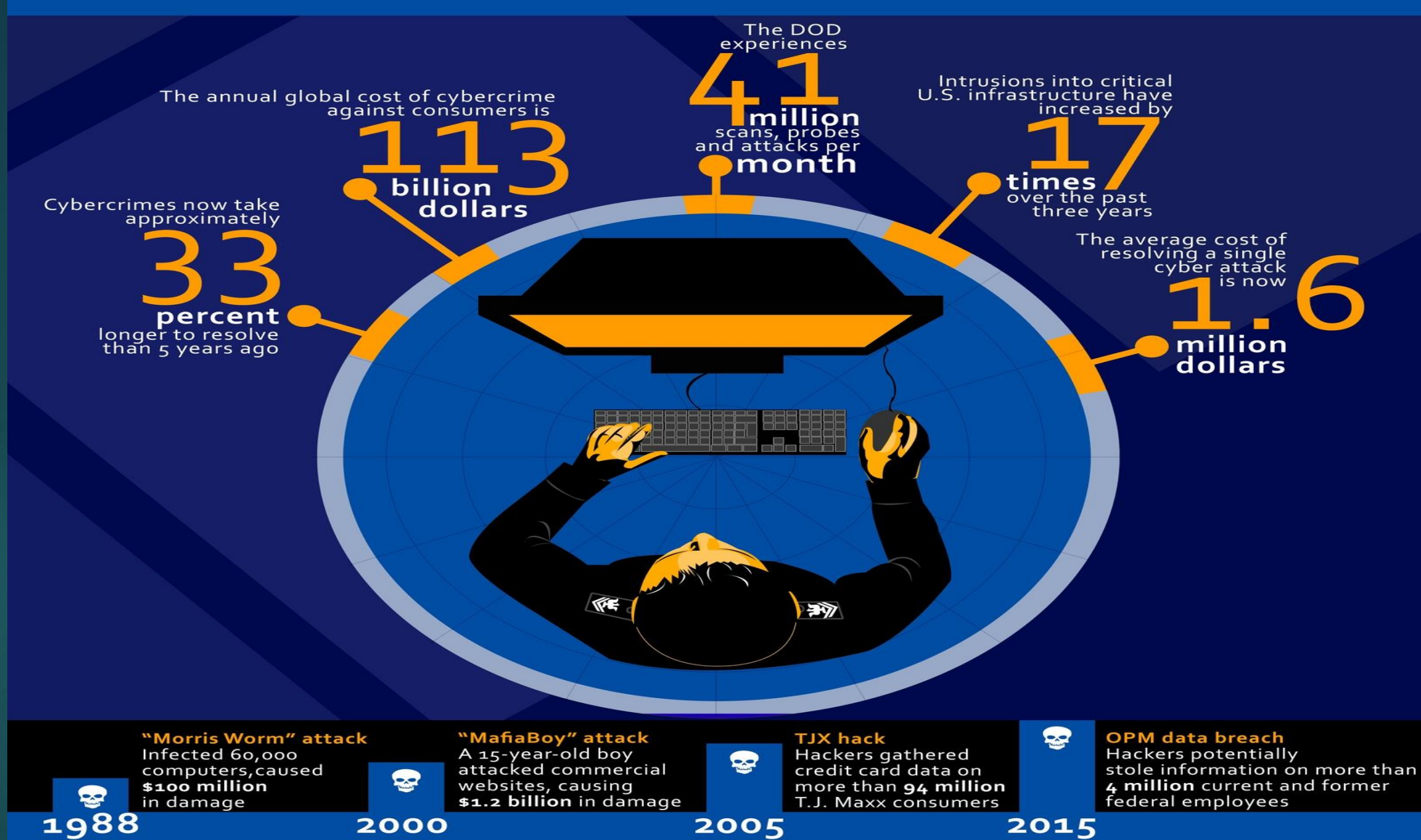
VIRUSES AND MALWARE

INSTRUCTOR: DANIEL CHONG
EMAIL: dchong@mybpl.org

COURSE OBJECTIVE: TO CULTIVATE AN UNDERSTANDING OF HOW YOU CAN PROTECT YOUR COMPUTER, WHILE BROWSING THE INTERNET, FROM VIRUSES AND MALWARE.

Outline:

- ▶ Viruses and Malware, What Are They?
- ▶ Common Types of Malware and Viruses
- ▶ Common Ways People Infect Their Computer(s)
 - ▶ High Risk Websites
- ▶ How To Tell If You've Been Infected With Malware
- ▶ Preventative Measures
 - ▶ Anti-Virus Software
 - ▶ Follow-Along Scan (Malwarebytes)
 - ▶ Ad-Blocker
 - ▶ Firewalls
 - ▶ Link Safety and Good Password Habits
 - ▶ Backup, Backup, Backup!
- ▶ Q/A



Information taken from the Cyber Warfare Division of the United States Navy
 Author: Austin Rooney

Viruses and Malware, What Are They?

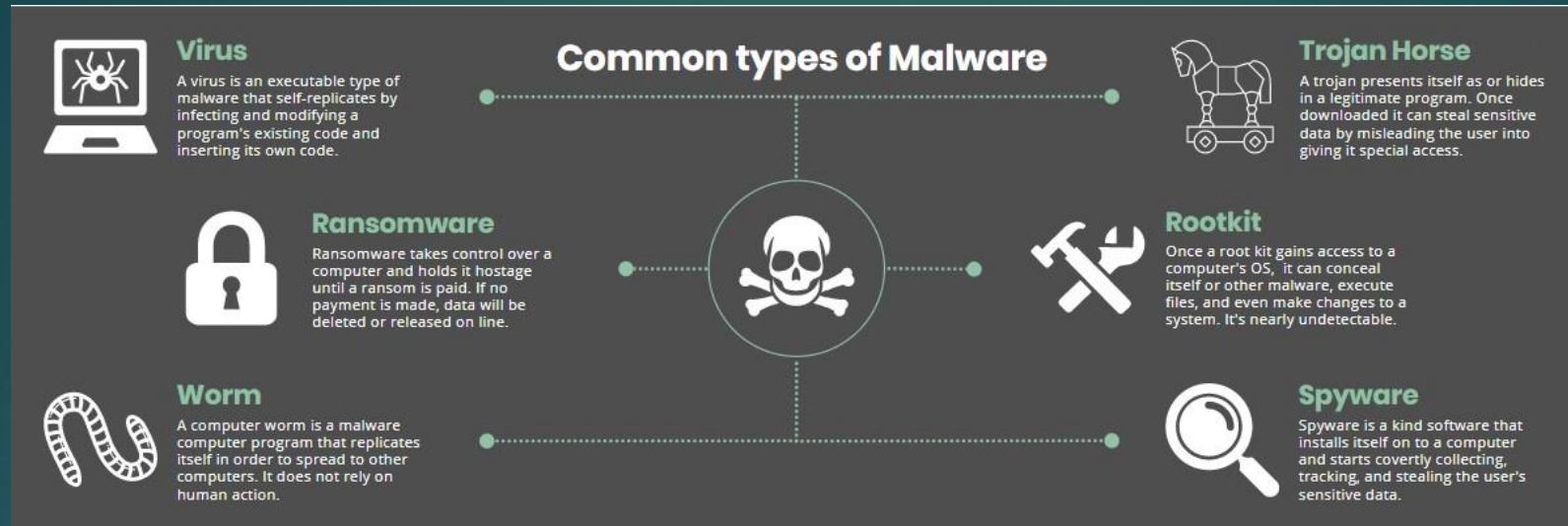
Back when the Personal Computer was becoming a common household item, the term for anything that could negatively affect your computer was a **VIRUS**. There were many different types of viruses but it encompassed every sort.

Today, a virus has become a subsection of a broader term called **MALWARE**. Malware is a blanket term for Malicious Software, but these types of software can be broken down into, more specifically, two categories.

- ▶ Infection and Delivery Methods
- ▶ Actions



Common Types of Malware and Viruses



Infection and Delivery Methods

- ▶ Virus
- ▶ Worm
- ▶ Trojan
- ▶ Drive-by Download
- ▶ Email Phishing*

Malware Actions

- ▶ Adware*
- ▶ Spyware
- ▶ Ransomware
- ▶ Scareware
- ▶ Rootkit

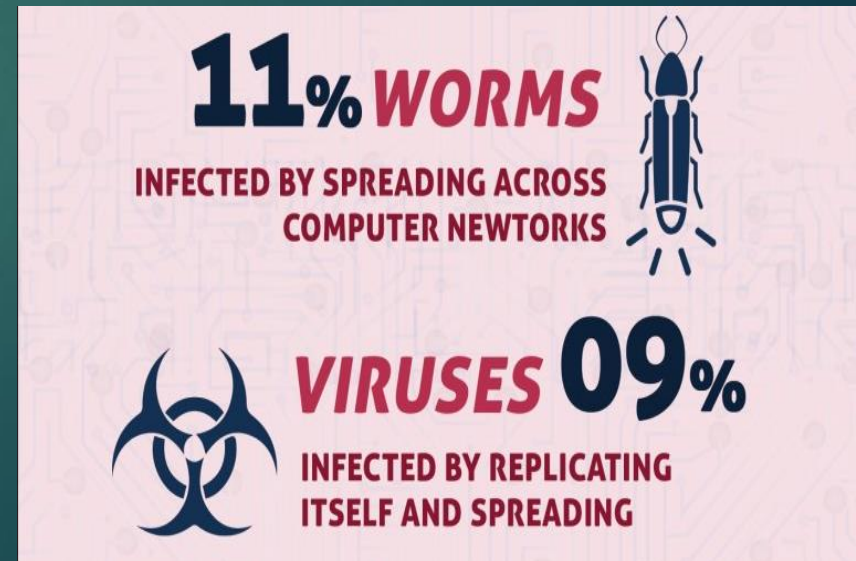
Viruses and Worms

VIRUS: This is a type of program that appends itself to another Program or File and from there self-replicates until it has completely taken over the system; even taking over other computers on the network.

One especially common one is called a **MACRO-VIRUS**, and this specifically attacks and corrupts Microsoft Office applications and file types.

WORM: Another type of self-replicating program, but instead of attaching itself to a specific part of your system, it is generally a small, independent program that will run in the background of your system processes.

It is most commonly used to turn your computer into a “Bot” on a Bot (Zombie) Net.



Statistics taken from:
NetworkSupport.com

Trojan

A **TROJAN** is considered to be malware that masquerades as a utility or program that will improve the Quality of Life for your computer. It is named after the fabled Trojan Horse that appeared as a gift, but instead carried a dangerous payload.

This type of malware is generally given permission by the User to install itself on the system!



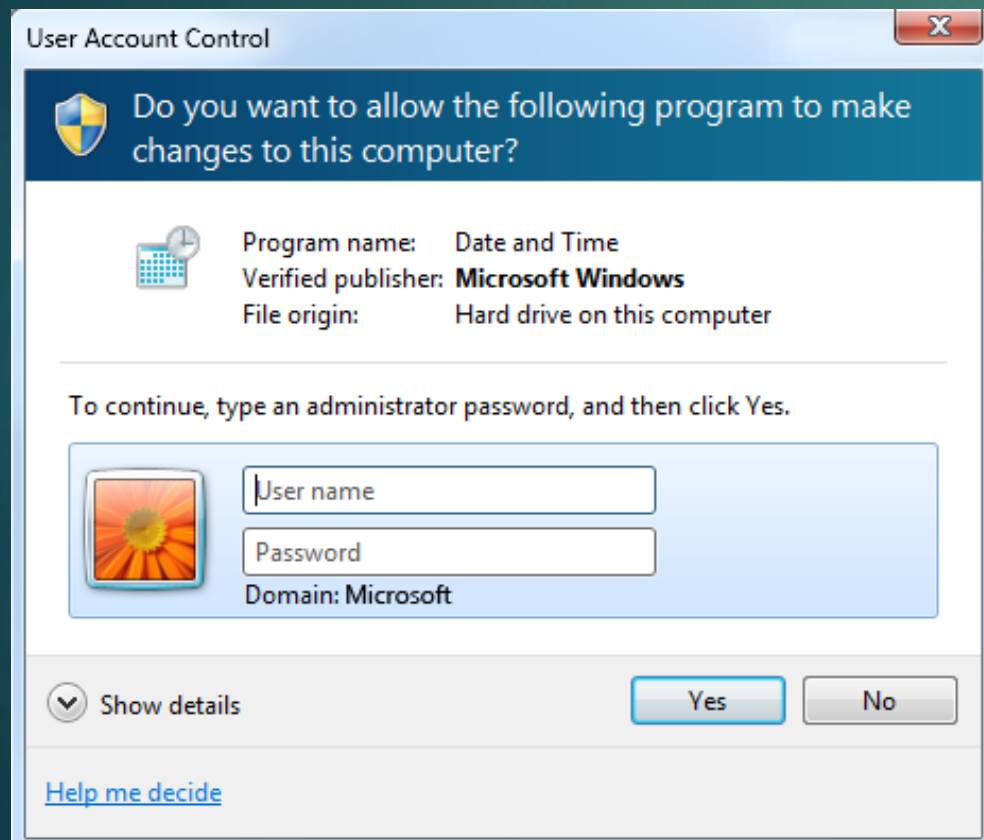
Statistics taken from:
NetworkSupport.com



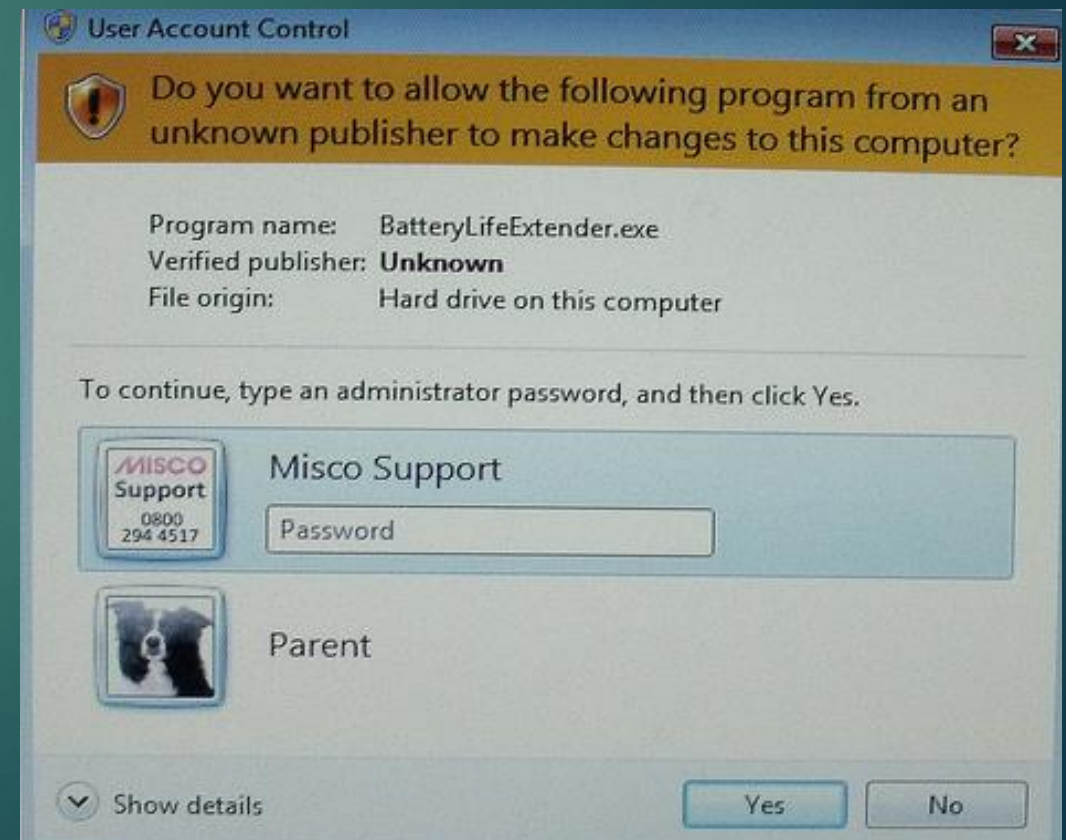
Trojans Continued...

Always Make sure to check if you are downloading a piece of software from a verified publisher! Make Sure you can trust it, and run it through your anti-virus software.

Trusted



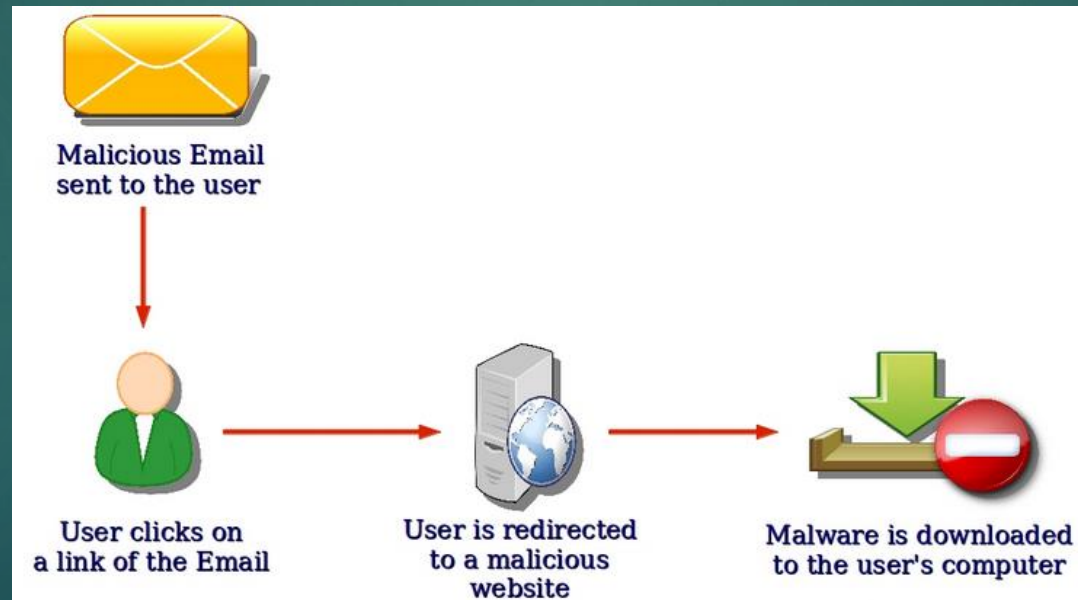
Suspicious



Drive-by Downloads

A **DRIVE-BY DOWNLOAD** is probably the most common way a computer will become infected with malware. It occurs when you visit a bad webpage or are redirected there from a malicious link in an email.

The webpage(s) will exploit a weakness in your browser and infect your system.



Email Phishing

EMAIL PHISHING has always been one of the most common cyber-security attacks, and while it is not necessarily tied together with malware, it can be used to deliver it. (i.e. **DRIVE-BY DOWNLOAD**)

Usually Phishing is attempting to get your personal information; be it login info, credit card numbers, social security etc.

If you received an unsolicited email that is supposedly from your bank asking you to "verify your information" then you are probably the target of a phishing attack. Always navigate to a banking website yourself, never trust a link to one.

The screenshot shows an email interface with the following details:

- From:** Amazon <management@mazoncanada.ca> on behalf of Amazon (Note: "management@mazoncanada.ca" is circled in red, with an arrow pointing to the text "not an Amazon email address (note the missing A in Amazon)").
- To:** @sheridanc.on.ca
- Cc:**
- Subject:** Suspension

The email body features the Amazon.com logo at the top. Below it, the text "Dear Client," is circled in red, with an arrow pointing to the text "Generic non-personalized greeting".

The main body text reads: "We have sent you this e-mail, because we have strong reason to believe, your account has been used by someone else. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it."

Below this text, a line of text says "To confirm your identity with us click the link bellow:". The link "<https://www.amazon.com/exec/obidos/sign-in.html>" is circled in red. An arrow points from this link to the text "Hovering over the link reveals it points to a non-Amazon site - 'http://redirect.kereskedj.com'".

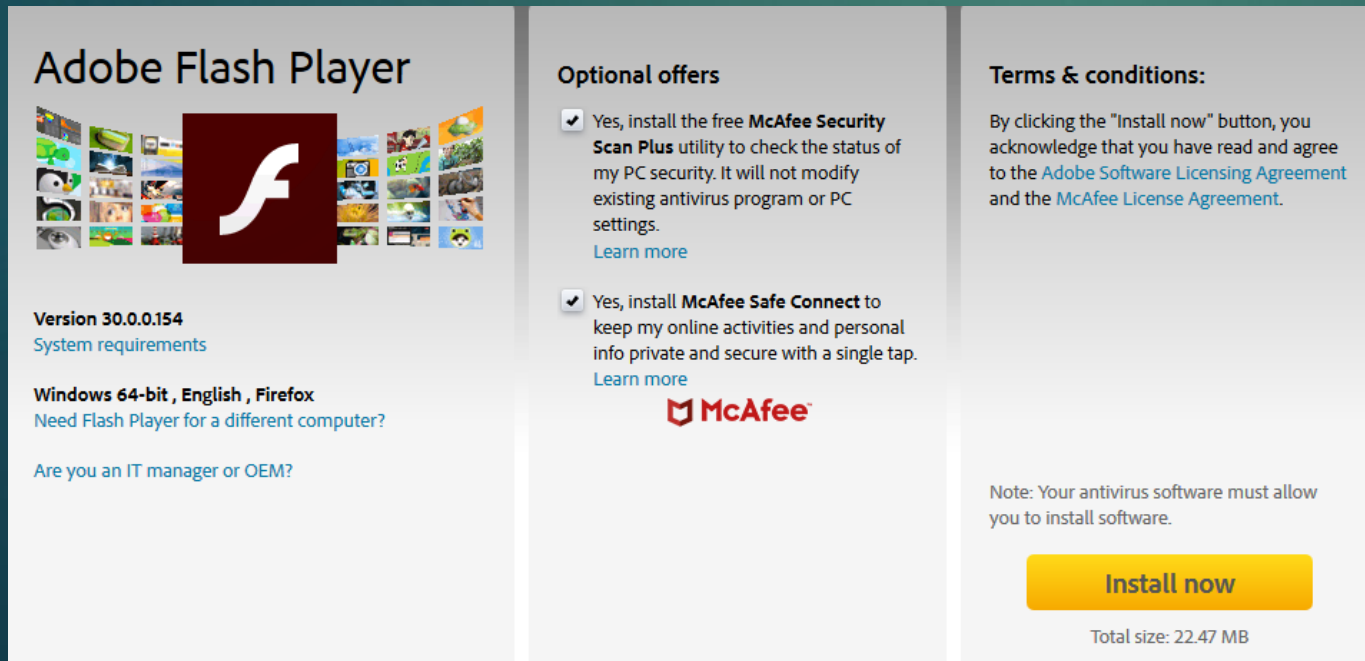
The email concludes with "Sincerely, The Amazon Associates Team" and a small Amazon logo in the bottom right corner. At the very bottom, it says "© 1996-2013, Amazon.com, Inc. or its affiliates".

Adware

ADWARE, while not truly malware in the conventional sense, can be very annoying to deal with, especially as it is generally given permission by the user to be on the system.

This type of software uses some form of advertising delivery system. And is generally bundled together with legitimate software. Even major companies will serve you up adware.

Generally it can be removed by uninstalling the software it can with .



Adobe Flash Player

Version 30.0.0.154
[System requirements](#)

Windows 64-bit , English , Firefox
[Need Flash Player for a different computer?](#)

[Are you an IT manager or OEM?](#)

Optional offers

- Yes, install the free **McAfee Security Scan Plus** utility to check the status of my PC security. It will not modify existing antivirus program or PC settings.
[Learn more](#)
- Yes, install **McAfee Safe Connect** to keep my online activities and personal info private and secure with a single tap.
[Learn more](#)

McAfee

Terms & conditions:

By clicking the "Install now" button, you acknowledge that you have read and agree to the [Adobe Software Licensing Agreement](#) and the [McAfee License Agreement](#).

Note: Your antivirus software must allow you to install software.

Install now

Total size: 22.47 MB



Java Setup

Java™ ORACLE™

We recommend installing the FREE Browser Add-on from Ask

Search + Ask Facebook Listen to Music Amazon YouTube

Get the best of the Web delivered to you!

Receive Facebook status updates directly in your browser, listen to thousands of top radio stations, and get easy access to search, YouTube videos, local weather, and news. Supports Internet Explorer, Google Chrome and Mozilla Firefox.

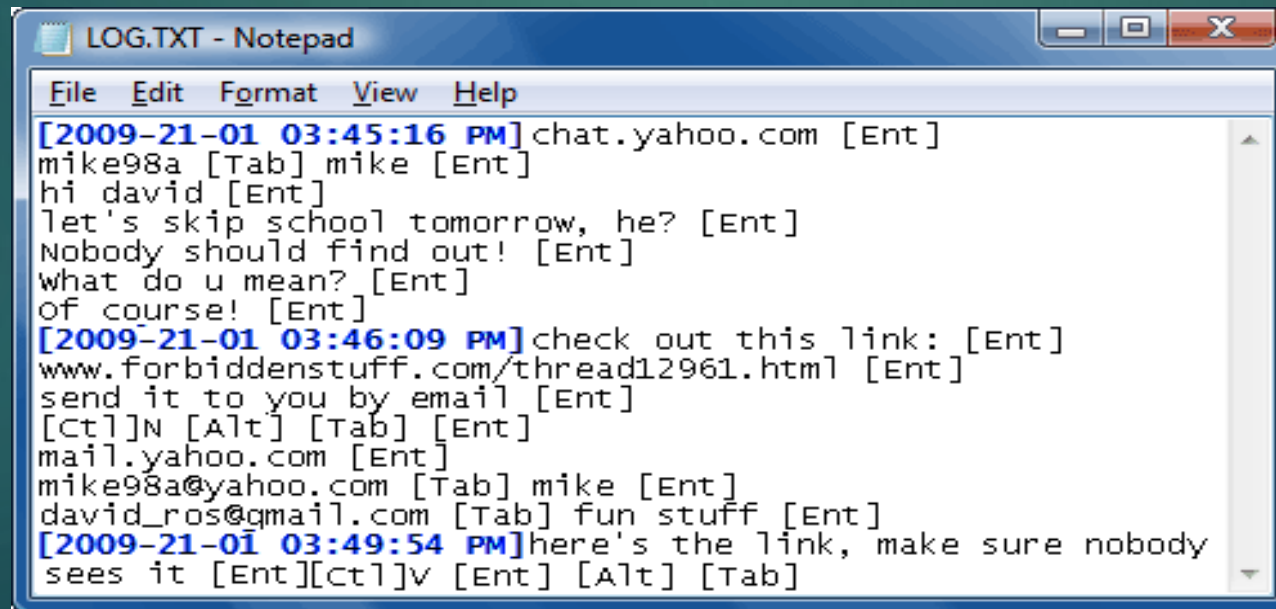
Install the Ask Toolbar and make Ask my default search provider

By installing this application and associated updater from Ask.com, your use is subject to the [Ask.com Terms and Conditions](#) and [Privacy Policy](#).

Cancel Next >

Spyware

SPYWARE will monitor your computer and reveal collected information to the interested party. This can be benign when it tracks what webpages you visit (i.e. cookies), or it can be incredibly invasive when it monitors EVERYTHING you do with your mouse and keyboard.



```
LOG.TXT - Notepad
File Edit Format View Help
[2009-21-01 03:45:16 PM] chat.yahoo.com [Ent]
mike98a [Tab] mike [Ent]
hi david [Ent]
let's skip school tomorrow, he? [Ent]
Nobody should find out! [Ent]
what do u mean? [Ent]
Of course! [Ent]
[2009-21-01 03:46:09 PM] check out this link: [Ent]
www.forbiddenstuff.com/thread12961.htm [Ent]
send it to you by email [Ent]
[Ctrl]N [Alt] [Tab] [Ent]
mail.yahoo.com [Ent]
mike98a@yahoo.com [Tab] mike [Ent]
david_ros@gmail.com [Tab] fun stuff [Ent]
[2009-21-01 03:49:54 PM] here's the link, make sure nobody
sees it [Ent][Ctrl]v [Ent] [Alt] [Tab]
```

Ransomware

RANSOMWARE has lately become very popular way for cyber-criminals to make money and it is only becoming more common.

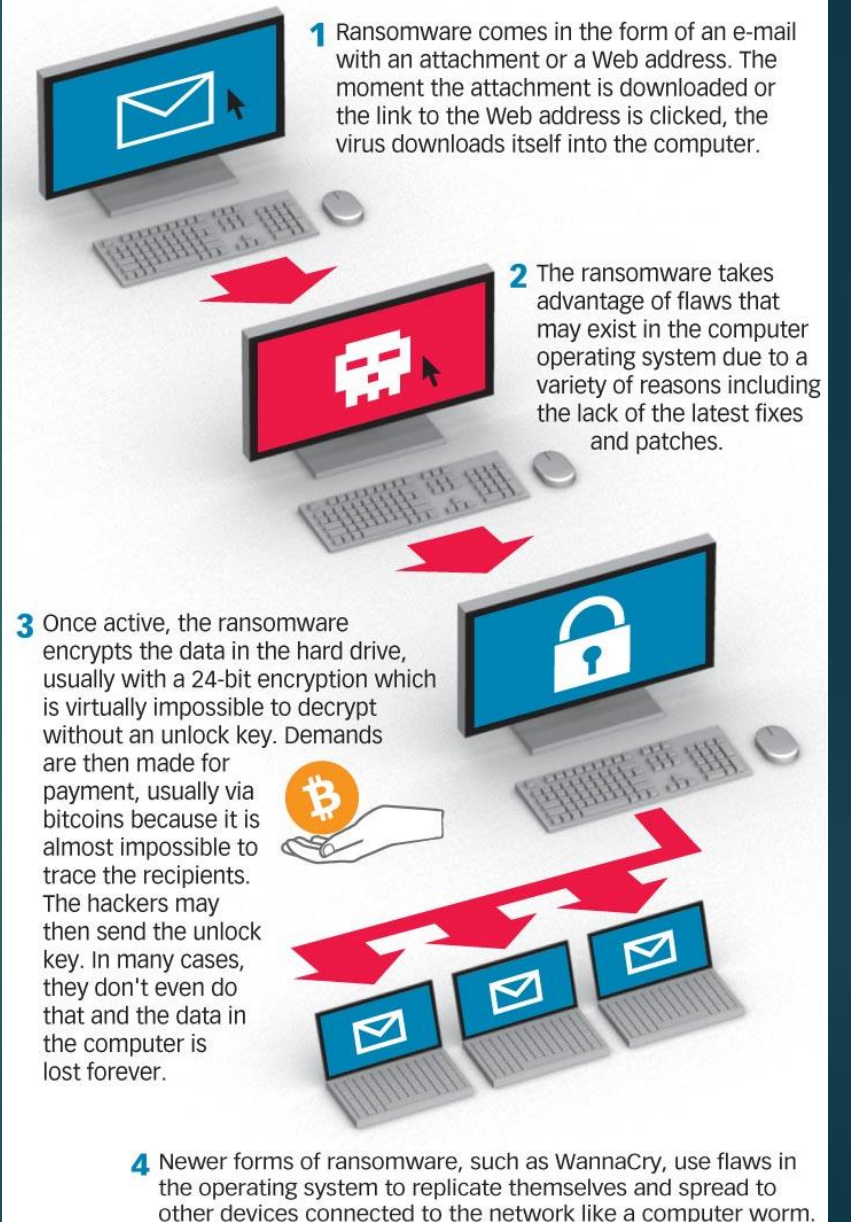
This is the MOST SERIOUS type of malware out there. It is extremely difficult to remove.

It alters your system in such a way that you are unable to get into it normally. This is usually done by encrypting files.

The cyber-criminal will then hold your files hostage and ransom them back to you for outrageous prices (usually asked for in Bitcoin or another crypto-currency).

Newer types of ransom ware will replicate themselves over a network, attacking all computers that are connected.

How ransomware works





Ooops, your files have been encrypted!

English

Payment will be raised on

5/15/2017 15:58:08

Time Left

02:23:58:59

Your files will be lost on

5/19/2017 15:58:08

Time Left

06:23:58:59

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

CMT from Mondays to Fridays



Send \$300 worth of bitcoin to this address:

115p7UMMngoj1pMvvpHijcRdfJNXj6LrLn

Copy

Scareware

SCAREWARE is generally a type of utility software that appears to be something legitimate (not unlike a **TROJAN**), often claiming that it could speed or clean up your computer. When it actually runs it tells you that your computer is broken in some way; usually in very scary, technical terminology.

The software then claims that it can fix your problems if you pay them for their services.

Some of these services can be posing as legitimate businesses.



Scareware Continued...

Another form of **SCAREWARE** are false accusations from the “FBI” or some other government agency, sometimes even corporations like Microsoft or Apple.

These will generally lock your computer with a screen that tells you that there are warrants for your arrest and your computer has been locked as evidence. They will demand you pay them to get access to your computer back.

Know that a Government Agency needs a warrant to do anything to your personal property and would not contact you by locking your computer.

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of \$200.

You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through [REDACTED]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [REDACTED] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).



[REDACTED]

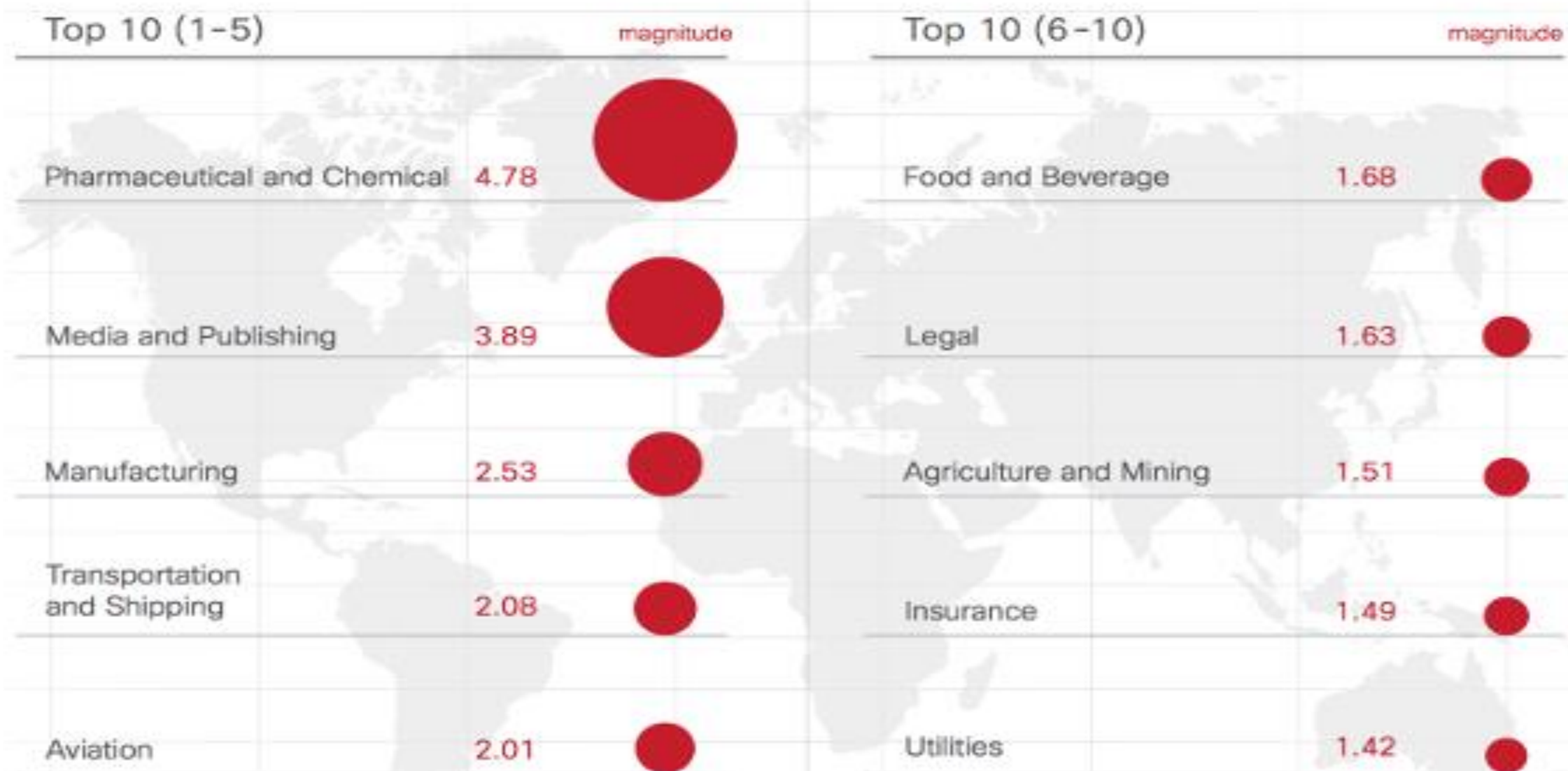
OK

Common Ways People Infect Their Computer

There are many different ways that your computer system could become infected with malware. Some of the most common are:

- ▶ Permission is given by the User!
- ▶ Phishing Attempts/Malicious Email
- ▶ Bad Link
- ▶ Outdated Programs (i.e. Adobe Flash or Java)
- ▶ Downloading Movies or Music via Torrent Websites
- ▶ Free Streaming Websites
- ▶ Compromised USB Drives (Common within Corporations)

Figure 9. Vertical Risk of Web Malware Encounters, All Regions, January 1 - November 15, 2014



How To Tell If You've Become Infected With Malware

There are some tell-tale signs that your computer has become infected with malware, but don't let that fool you!

Although, sometimes your system could be running perfectly normal and you could still have malware installed on your computer. If your computer exhibits any of these symptoms then you most likely have malware.

- You receive Ransom Demands. (Ransomware)
- Significant decrease in performance/speed. (General Malware)
- Popups Everywhere!!! (Adware)
- Keep getting redirected to random webpage(s). (Adware)
- An Unknown App keeps sending system messages i.e. "YOUR COMPUTER IS INFECTED WITH 1,502 MALICIOUS PROGRAMS! CLICK HERE >>>> TO CLEAN YOUR INFECTED SYSTEM!" (Scareware)
- Mysterious posts to social media accounts with links attached. (Spyware)
- System Tools are unresponsive. (Rootkit)



Preventative Measures

The best way to prevent malware is YOU! By keeping a watchful eye and practicing safe browsing habits you will be able to prevent MOST malware that you see today.

Now that doesn't mean you shouldn't be vigilant and take every step you can to secure your computer.

Tonight we will be going over three ways you can keep your computer secure

- ▶ Anti-Virus Software
- ▶ Ad-Blocker
- ▶ Link Safety



Anti-Virus Software

Anti-Virus software is designed to prevent, detect and remove malicious software and potentially unwanted programs (PUPS).

Anti-Virus uses signature based detection methods to scan your system for malware code patterns (signatures/thumbprints).

Malware Definitions (known malware types) are updated regularly, but new malware is being created everyday and no Anti-Virus is 100% secure.

Windows Defender is the stock Anti-Virus that comes preloaded on all Windows 10 Machines. It will be enough, provided you are practicing safe browsing habits, 9 times out of 10.

Third Party Anti-Virus software comes in a myriad of different forms, most offer free versions while also offering premium versions.

Third Party software can be compared here: <https://www.av-test.org/en/antivirus/home-windows/>



Ad-Blocker

In today's day and age we are constantly bombarded with ads, some of these ads can be malicious! So why not protect yourself with an ad-blocker? You can add these extensions on to any browser and most are free-open source software that is released to the public.

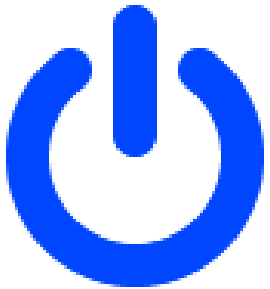
The overall best rated ad-blocker is called **uBlock Origin**.

Along with ad-blockers you can also use anti-tracking extensions (Privacy Badger) or even some that will not allow any sort of script run over the internet without your permission (NoScript).

Note: Anti-Script Extensions can sometimes “break” the webpage you are viewing. Although they make your computer secure by not allowing any sort of JavaScript to run on your computer, many websites rely on JavaScript to present their content to you.

This is where the fine line of convenience and security meet.

uBlock Origin 1.16.16



⚡ ✍️ 📄 ☰

requests blocked

on this page
78 or 10%

since install
213,552 or 39%

domains connected

12 out of 13

📄 📺 🛡️ A

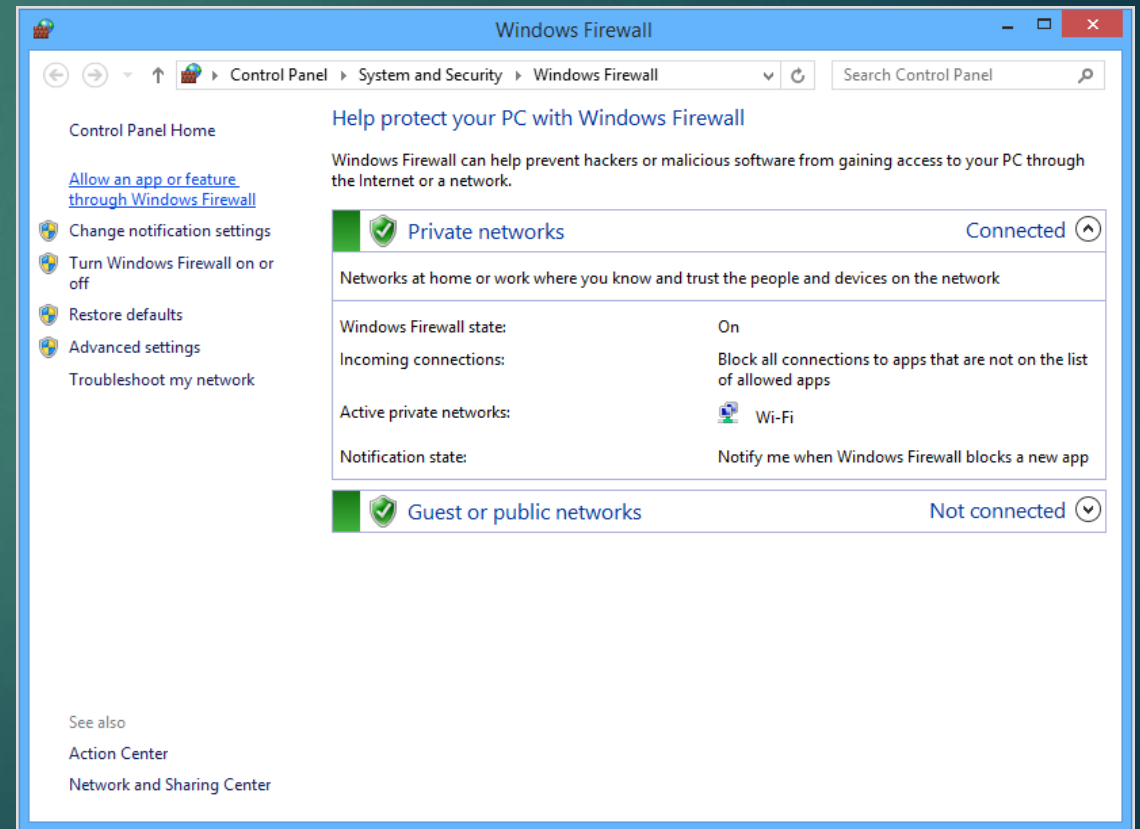
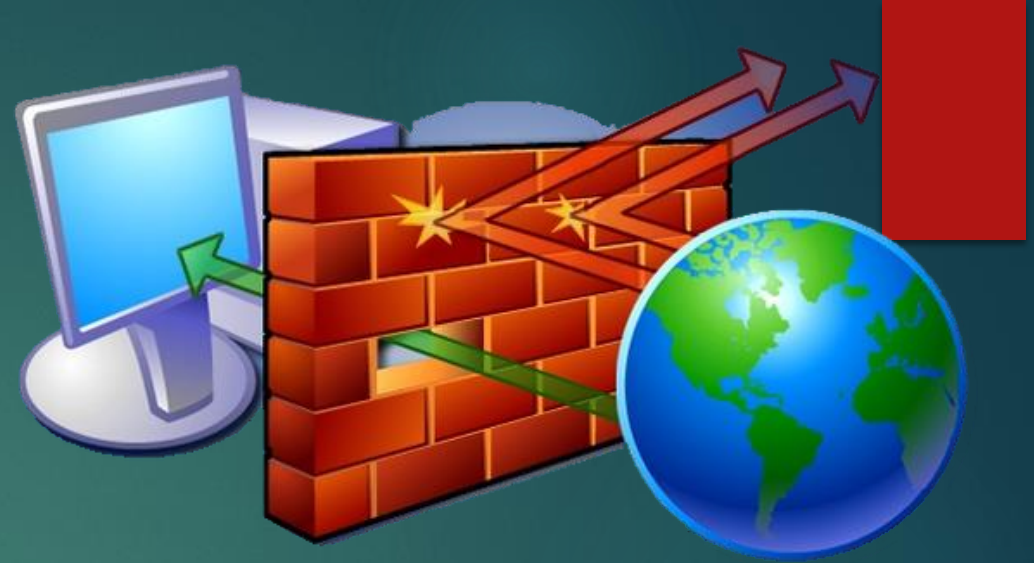
Firewalls

Think of a firewall as a filter. It keeps malicious programs separated from your system so it doesn't even have the chance to attack.

- It does this by either letting parts of a program work, or none at all.

Windows Firewall comes standard on all Windows devices.

Most routers and PREMIUM Anti-Virus Software will come with some sort of firewall configuration.



Link Safety & Good Password Habits

All of these Links go to the same place!

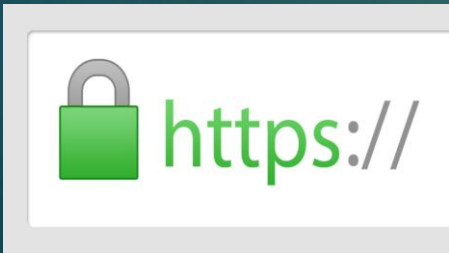
<https://global.sitesafety.trendmicro.com/LinkRolexwatch.net>

Watch out for shortened Links!

<https://bit.ly/1NwiXXn>
<http://checkshorturl.com/>

Keep an eye out for Country Codes! (Pg. 9)

Always look for the lock, if you are doing something such as online shopping or banking.



Browser add-ons such as HTTPSEverywhere will automatically place you on secure browser (HTTPS) if the website supports it.

Keep Secure with a good Password or better yet a Passphrase.

Easy passwords to break have to do with important things from your life, things you might mention on social media or your birthday.

Weak: kipa52893

Hard passwords to break have nothing to do with anything, the best way to make a secure password is to pick three words and add a combination of special characters and numbers.

Strong: jello#Surfing82m0tHer*9

Browser add-ons such as LastPass can be used to store passwords and is accessed by a master password. This can be used to make long strings of numbers and characters your password without having to remember them.

- Note: This is advanced, only use after thorough research on how it works.

Password Do's and Don'ts



DATA BREACHES ARE BECOMING COMMON

707.5
million records
compromised in 2015

40% of data breaches are due to weak or stolen passwords. In 2015, 781 data breaches were reported in the U.S. Keep your personal and business information safe with these password tips.

MOST COMMON PASSWORDS

- 1 123456
- 2 password
- 3 12345678
- 4 qwerty
- 5 12345



Over 65% of passwords are too simple and easy to crack

NEVER MAKE THESE MISTAKES

- use important dates from your life
- use sequential or repetitive number strings
- use the same password for multiple accounts
- Keep the same password for more than a month

PASSWORD CREATION GUIDELINES



- Use more than 12 characters
- Use upper and lower case
- Use special characters

Backup, Backup, Backup!



BACKUP

RECOVER

RESTORE

“Save for a rainy day, you’ll never know when you’ll need it.”

Create a System Restore Point!

Go to the Windows Search Bar >> type in System Restore >> Follow the Wizard Setup

Prevent your important files from being lost by backing them up. This will help you keep moving even if you are a victim of a malware attack, or even hardware failure.

Options for backing up your files include: External Hard Drives (hardware option) and Cloud Storage Services (software option).

External Hard Drives are the most reliable! Encrypt Them!

Cloud Services can be a good way to store your files for free, usually up to 15GB, but are also susceptible to auto-syncing encrypted or corrupted files to the cloud.

Q/A

Thanks for joining me! Please do not hesitate to email me if you ever have any questions.

I can be reached at dchong@mybpl.org

Stay Safe!