Cybersecurity Threats

What is cybercrime?

- *Cybercrime is defined as a crime where a computer is the object of the crime or is used as a tool to commit an offense. A cybercriminal may use a device to access a user’s personal information, confidential business information, government information, or disable a device.*

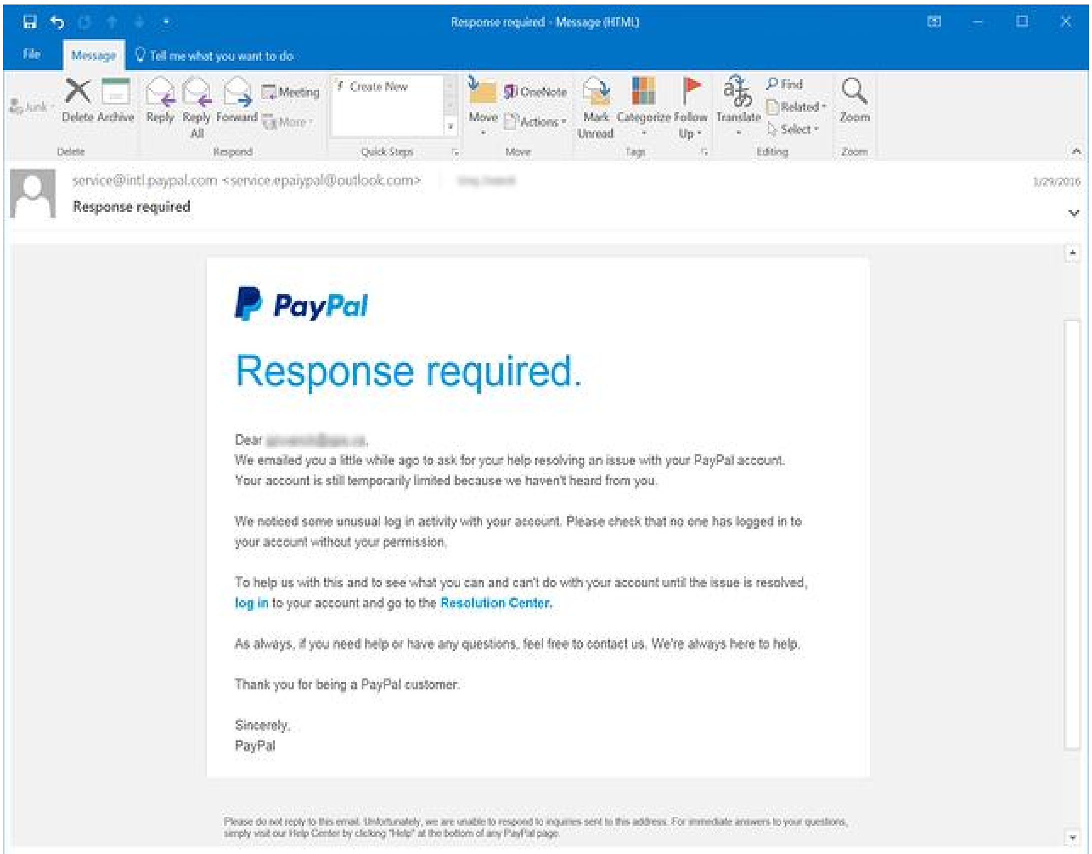
❖ TYPES OF CYBERCRIME

1. **Personal Cybercrime**
   - **Harassment**
     1. Cyberbullying: between two minors
     2. Cyber-harassment: between adults
     3. Cyber-stalking:
        - More serious in nature
        - Stalker demonstrates a pattern of harassment
        - Poses a credible threat of harm

Personal cybercrime is perpetrated against individuals, as opposed to businesses and other organizations. These are crimes that affect you directly and that you need to be aware of. Cyberbullying and cyber-stalking are two categories of harassment. When the exchange involves two minors, it is cyberbullying; when it involves adults, it is cyber-harassment. Cyber-stalking is more serious in nature, with the stalker demonstrating a pattern of harassment and posing a credible threat of harm.

- **Phishing**
  - ✓ Email messages and IMs
  - ✓ Appear to be from someone with whom you do business

- ✓ Designed to trick you into providing usernames and passwords



service@intl.paypal.com <service.epaiypal@outlook.com> [redacted] 1/29/2016

Response required

PayPal

Response required.

Dear [redacted],
We emailed you a little while ago to ask for your help resolving an issue with your PayPal account.
Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

As always, if you need help or have any questions, feel free to contact us. We're always here to help.

Thank you for being a PayPal customer.

Sincerely,
PayPal

Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help" at the bottom of any PayPal page.

Figure 1. A Phishing attack mimicking the email from Paypal

(source: https://www.phishing.org/phishing-examples)

- **Pharming**
  - ✓ is a cyberattack intended to redirect a website's traffic to another, fake site. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software.
  - ✓ Redirects you to a phony website **even if you type the URL**
  - ✓ Hijacks a company’s domain name
  - ✓ Pharming has been called "phishing without a lure."

Figure 2 below shows an example of pharming wherein the person browsing and using the search engine “Google” was redirected to a different site.

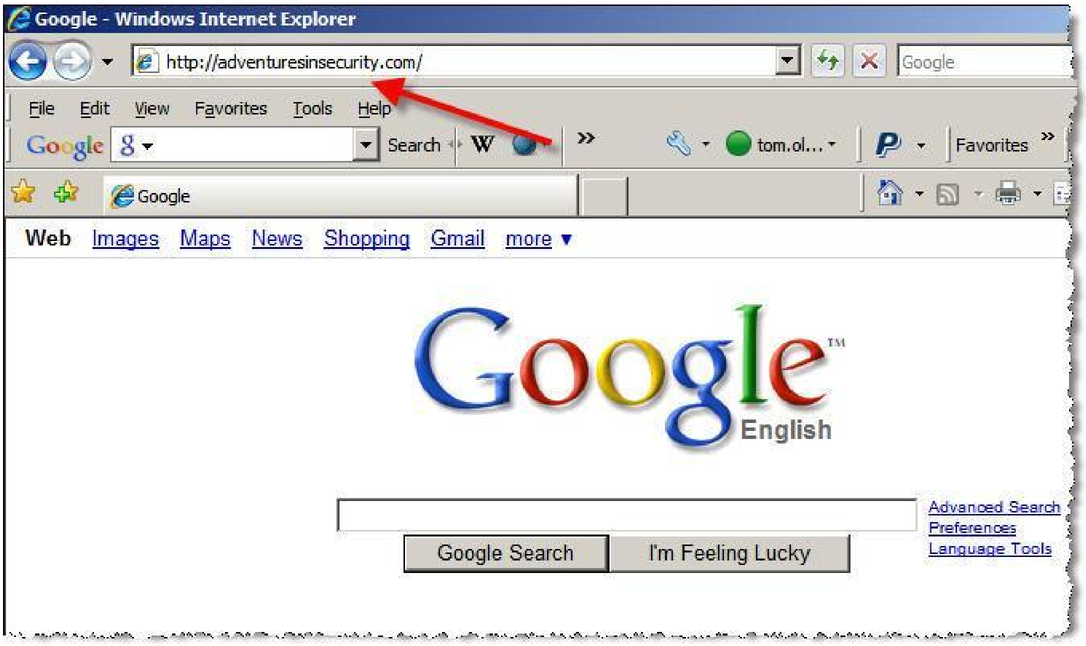

Google - Windows Internet Explorer
http://adventuresinsecurity.com/
Google
File Edit View Favorites Tools Help
Google
Search
W
tom.ol...
Favorites
Google
Web Images Maps News Shopping Gmail more ▾
Google™
English
Advanced Search
Preferences
Language Tools
Google Search
I'm Feeling Lucky

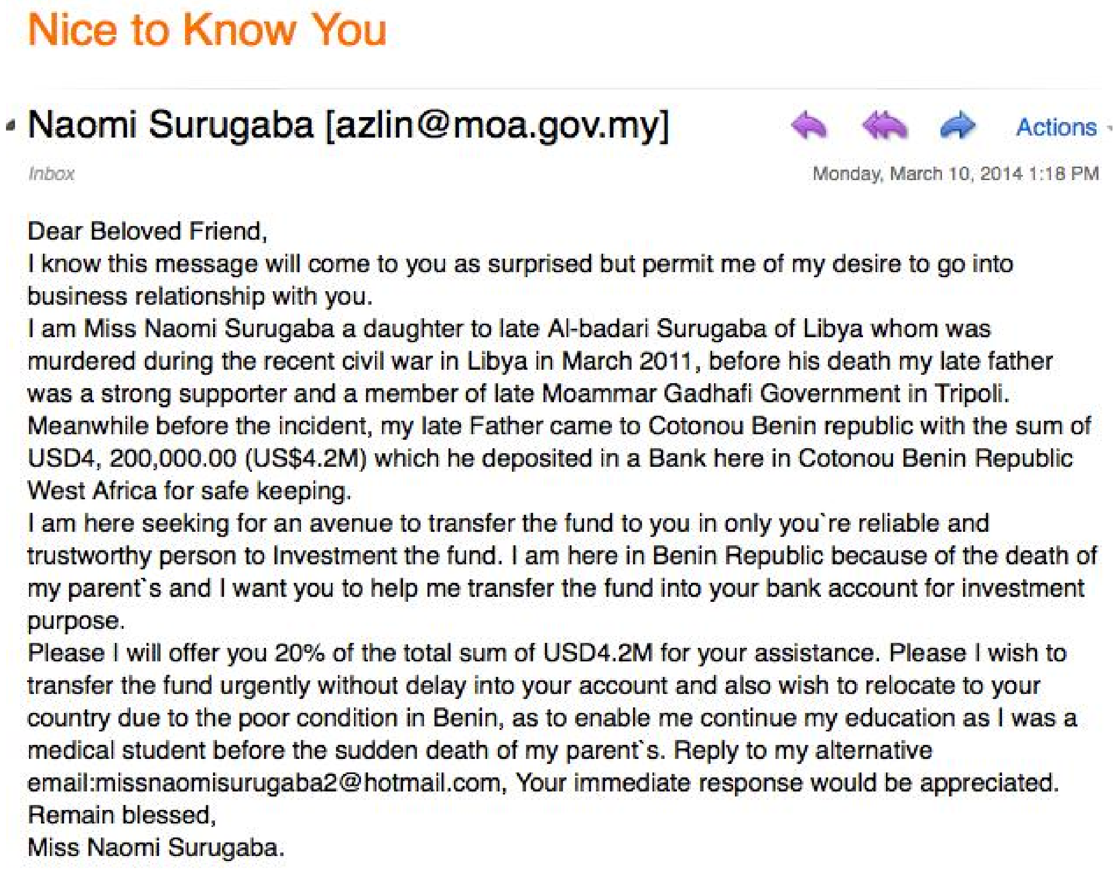
Figure 2. A Pharming attack mimicking the Google search engine

(source: https://wpree94800.weebly.com/section-6---effects-of-ict/pharming)

In phishing, the perpetrator sends out legitimate-looking e-mails, appearing to come from some of the Web's most popular sites, in an effort to obtain personal and financial information from individual recipients. But in pharming, larger numbers of computer users can be victimized because it is not necessary to target individuals one by one and no conscious action is required on the part of the victim. In one form of pharming attack, code sent in an e-mail modifies local host files on a personal computer. The host files convert URLs into the number strings that the computer uses to access Web sites. A computer with a compromised host file will go to the fake Web site even if a user types in the correct Internet address or clicks on an affected bookmark entry. Some spyware removal programs can correct the corruption, but it frequently recurs unless the user changes browsing habits.

2. Social Network Attacks

- **Adware** – an unwanted software designed to throw advertisements up on the screen of the user’s computer while browsing the social networking sites.
- **Clickjacking** – clicking on a link allows this malware to post unwanted links on the web page.
- **Malicious script scams** – copy and paste some text into your address bar, which executes a malicious script that creates pages and events or sends spam to your friends.
- **Fraud**
  - ✓ could involve hiding of information or providing incorrect information for the purpose of tricking victims out of money, property, and inheritance.
  - ✓ schemes that convince you to give money or property to a person
- **Shill bidding**
  - ✓ fake bidding to drive up the price of an item


Nice to Know You
Naomi Surugaba [azlin@moa.gov.my]
Actions
Inbox
Monday, March 10, 2014 1:18 PM

Dear Beloved Friend,
I know this message will come to you as surprised but permit me of my desire to go into business relationship with you.
I am Miss Naomi Surugaba a daughter to late Al-badari Surugaba of Libya whom was murdered during the recent civil war in Libya in March 2011, before his death my late father was a strong supporter and a member of late Moammar Gadhafi Government in Tripoli.
Meanwhile before the incident, my late Father came to Cotonou Benin republic with the sum of USD4, 200,000.00 (US$4.2M) which he deposited in a Bank here in Cotonou Benin Republic West Africa for safe keeping.
I am here seeking for an avenue to transfer the fund to you in only you`re reliable and trustworthy person to Investment the fund. I am here in Benin Republic because of the death of my parent`s and I want you to help me transfer the fund into your bank account for investment purpose.
Please I will offer you 20% of the total sum of USD4.2M for your assistance. Please I wish to transfer the fund urgently without delay into your account and also wish to relocate to your country due to the poor condition in Benin, as to enable me continue my education as I was a medical student before the sudden death of my parent`s. Reply to my alternative email:missnaomisurugaba2@hotmail.com, Your immediate response would be appreciated.
Remain blessed,
Miss Naomi Surugaba.

Figure 3. Example of online fraud

(source: https://heimdalsecurity.com/blog/top-online-scams//)

- **Identity Theft**
  - ✓ the crime of obtaining the personal or financial information of another person for the sole purpose of assuming that person's name or identity to make transactions or purchases.

3. Cybercrime Against the Government

- ○ **Hacking –** *is an attempt to exploit a computer system or a private network inside a computer. Simply put, it is the unauthorized access to or control over computer network security systems for some illicit purpose. A computer hacker is* *a computer expert who uses their technical knowledge to overcome a problem. While **"hacker"** can refer to any skilled computer programmer, the term has become associated in popular culture with a "security hacker", someone who, with their technical knowledge, uses bugs or exploits to break into computer systems. **Hacktivism** is the act of misusing a computer system or network for a socially or politically motivated reason. Individuals who perform hacktivism are known as **hacktivists**. On the other hand, **data breach** is when a sensitive data was stolen or viewed by someone unauthorized.*

3 Types of Hacking

- **White-hat or "sneakers"** – Attempt to find security holes in a system to prevent future hacking
  - ✓ Also known as "ethical hackers," they're often employed or contracted by companies and governmental entities, working as security specialists looking for vulnerabilities. While they employ the same methods as black hat hackers, they always have permission from the system's owner, making their actions completely legal. White hat hackers implement strategies like penetration tests, monitor in-place security systems, along with vulnerability assessments. Ethical hacking, the term used to describe the nature of a white hat hackers' actions, can even be learned through independent sources, training, conferences, and certifications.
- **Black-hat or "crackers"** –Malicious intent such as theft and vandalism
  - ✓ Black hat hackers are normally responsible for creating malware, which is frequently used to infiltrate computerized networks and systems. They're usually motivated by personal or financial gain, but can also

participate in espionage, protests, or merely enjoy the thrill. Black hat hackers can be anyone from amateurs to highly experienced and knowledgeable individuals looking to spread malware, steal private data, like login credentials, along with financial and personal information. Upon accessing their targets and depending on their motives, black hat hackers can either steal, manipulate, or destroy system data.

- **Gray-hat** – Illegal but not malicious intent
  - ✓ As the name suggests, these individuals utilize aspects from black and white hat hackers, but will usually seek out vulnerabilities in a system without an owner's permission or knowledge. While they'll report any issues, they encounter to the owner, they'll also request some sort of compensation or incentive. Should the owner not respond or reject their proposition, a grey hat hacker might exploit the newfound flaws. Grey hat hackers aren't malicious by nature, but do seek to have their efforts rewarded. Since grey hat hackers don't have permission to access the system by its owner, their actions are ultimately considered illegal, despite any alarming findings they might reveal.

Common Hacking Tools

- **Rootkits –**a rootkit is a program or set of software tools that allow threat actors to gain remote access to control a computer system that interacts or connects with the internet. Originally, a rootkit was developed to open a backdoor in a system to fix specific software issues. Unfortunately, this program is now used by hackers to destabilize the control of an operating system from its legitimate operator or user.

There are different ways to install rootkits in a victim’s system, the most famous of them being social engineering and phishing attacks. Once rootkits are installed in the system, it secretly allows the hacker to access and control the system, giving them the opportunity to bring the system down or steal crucial data.

- **Keyloggers –** a specially designed tool that logs or records every key pressed on a system. Keyloggers record every keystroke by clinging to the API (application programming interface) when typed through the computer keyboard. The recorded file then gets saved, which includes data like usernames, website visit details, screenshots, opened applications, etc.

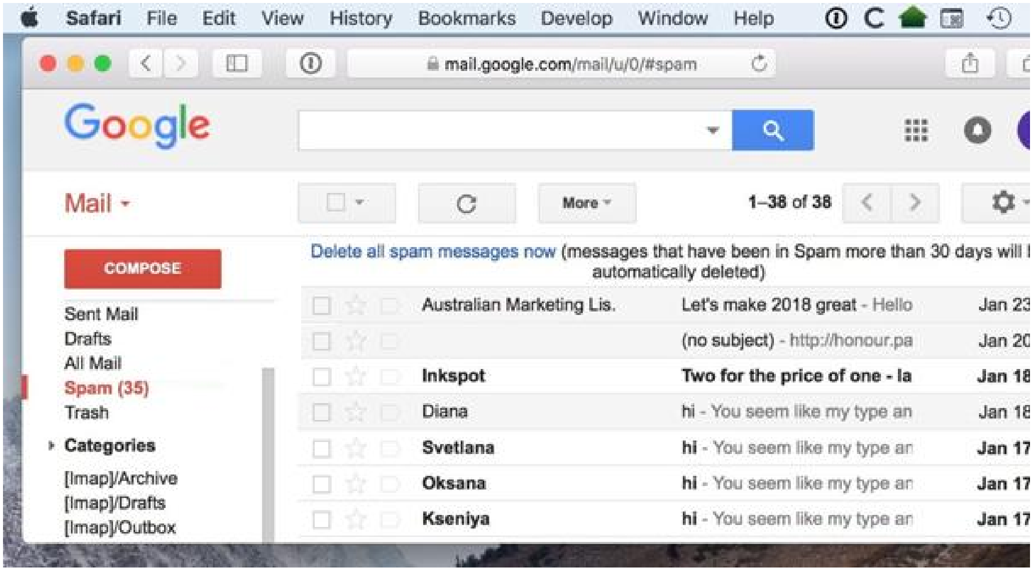
  Keyloggers can capture credit card numbers, personal messages, mobile numbers, passwords, and other details——as long as they are typed. Normally, keyloggers arrive as malware that allows cybercriminals to steal sensitive data.

- **Vulnerability Scanner** – classifies and detects various system weaknesses in networks, computers, communication systems, etc. This is one of the most common practices used by ethical hackers to find potential loopholes and fix them on an immediate basis. On the other hand, vulnerability scanners can also be used by black-hat hackers to check the system for potential weak spots in order to exploit the system.

- **Cyberterrorism**
  - *is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.*

Different Malwares

- **Spam** – a mass, unsolicited email. It is popular because it is easy and inexpensive to implement. Other forms include fax spam, IM spam, and text spam. The act of sending spam is called spamming.



Delete all spam messages now (messages that have been in Spam more than 30 days will b automatically deleted)

Australian Marketing Lis.	Let's make 2018 great - Hello	Jan 23
	(no subject) - http://honour.pa	Jan 20
Inkspot	Two for the price of one - la	Jan 18
Diana	hi - You seem like my type an	Jan 18
Svetlana	hi - You seem like my type an	Jan 17
Oksana	hi - You seem like my type an	Jan 17
Kseniya	hi - You seem like my type an	Jan 17

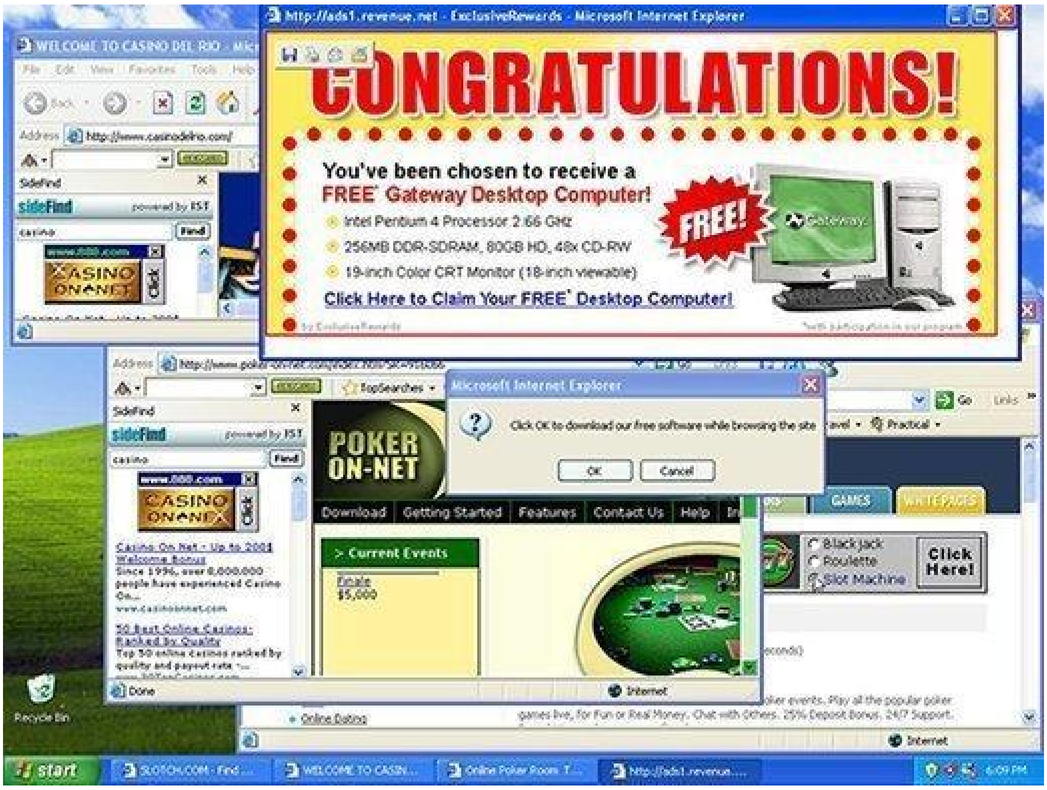
Figure 4. Spam messages in Gmail

(source: https://emailmate.com/blog/2019/06/gmail-spam-filter-working/)

- **Cookies** – A cookie is a small text file that allows the website to recognize the user and personalize the site. Although they are useful, they could be used to collect information that you do not want to share.

- ✓ Installed without your permission
- ✓ Help websites identify you when you return
- ✓ Track websites and pages you visit to better target ads
- ✓ May collect information you don’t want to share

- ○ **Adware** – shows you ads, usually in the form of pop-ups or banner ads in websites and in software. Ads generate income for the software developer. When these ads use CPU cycles and Internet bandwidth, it can reduce PC performance.



http://ads1.revenue.net - ExclusiveRewards - Microsoft Internet Explorer

CONGRATULATIONS!

You've been chosen to receive a FREE Gateway Desktop Computer!

- Intel Pentium 4 Processor 2.66 GHz
- 256MB DDR-SDRAM, 80GB HD, 48x CD-RW
- 19-inch Color CRT Monitor (18-inch viewable)

Click Here to Claim Your FREE Desktop Computer!

Microsoft Internet Explorer

Click OK to download our free software while browsing the site

Figure 5. Adware

(source: https://searchsecurity.techtarget.com/definition/adware)

- ○ **Spyware** –

- ○ **Virus** – is a program that replicates itself and infects computers. A computer virus needs a host file on which to travel, such as a game or email. The attack, also known as the payload, may corrupt or delete files, or it may even erase an entire disk. The virus uses the email program or game on the infected computer to send out copies of itself and infect other machines.

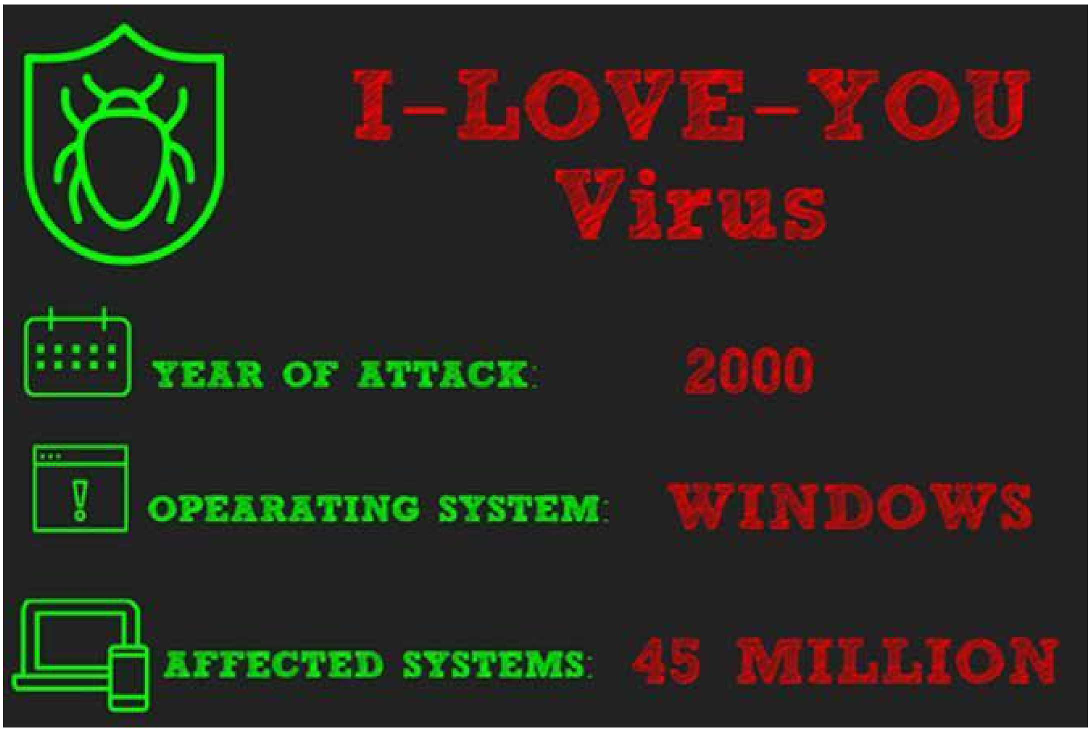


Figure 6. I Love You virus created by Filipinos

(source: https://infinitydatatel.com/computer-virus-protection-tips/)

The I love you computer virus emerged in May of 2000 and was a computer worm that infected millions of computers worldwide (approximately 10% of all computers were infected with the virus). U.S. governments had to take their messaging platforms off of the internet and maintain them locally to prevent infection of the virus. The Filipino creators used social engineering at its worst to send the file, which posed as a text file, but Windows had a vulnerability that did not show that it was, in fact, an *.EXE file. It would then email every single person on a user's contact list and overwrite numerous files with copies of itself, destroying computer systems.

○ **Logic Bomb**

✓ Behaves like a virus

- ✓ Performs malicious act
- ✓ Does not replicate
- ✓ Attacks when **certain conditions are met**

- ○ **Time Bomb**
  - ✓ A logic bomb with a trigger that is a specific time or date
    - April Fool's Day
    - Friday the 13th
    -

- ○ **Worms**
  - ✓ Self-replicating
  - ✓ Do not need a host to travel
  - ✓ Travel over networks to infect other machines
  - ✓ very dangerous as they take up a lot of bandwidth and other valuable resources.

There is no universal classification of computer worms, but they can be organized into types based on how they are distributed between computers. The five common types are as follows:

1. Internet Worms

Like they do with computer networks, computer worms also target popular websites with insufficient security. When they manage to infect the site, internet worms can replicate themselves onto any computer being used to access the website in question. From there, internet worms are distributed to other connected computers through the internet and local area network connections.

2. Email Worms

Email worms are most often distributed via compromised email attachments. They usually have double extensions (for example, .mp4.exe or .avi.exe) so that the recipient would think that they are media files and not malicious computer programs. When the victims click on the attachment, copies of the same infected file will automatically be sent to addresses from their contacts list.

An email message doesn’t have to contain a downloadable attachment to distribute a computer worm. Instead, the body of the message might contain a link that’s shortened so that the recipient can’t tell what it’s about without clicking on it. When they click on the link, they will be taken to an infected website that will automatically start downloading malicious software to their computer.

3. Instant Messaging Worms

Instant messaging worms are exactly the same as email worms, the only difference being their method of distribution. Once again, they are masked as attachments or clickable links to websites. They are often accompanied by short messages like “LOL” or “You have to see this!” to trick the victim into thinking that their friend is sending them a funny video to look at.

When the user clicks on the link or the attachment — be it in Messenger, WhatsApp, Skype, or any other popular messaging app — the exact same message will then be sent to their contacts. Unless the worm has replicated itself onto their computer, users can solve this problem by changing their password.

4. File-Sharing Worms

Although illegal, file-sharing and peer-to-peer file transfers are still used by millions of people around the world. Doing so, they are unknowingly exposing their computers to the threat of file-sharing worms. Like email and instant messaging worms, these programs are disguised as media files with dual extensions.

When the victim opens the downloaded file to view it or listen to it, they will download the worm to their computer. Even if it seems that users have downloaded an actual playable media file, an executable malicious file could be hidden in the folder and discreetly installed when the media file is first opened.

5. IRC Worms

Internet Relay Chat (IRC) is a messaging app that is mostly outdated nowadays but was all the rage at the turn of the century. Same as with today’s instant messaging platforms, computer worms were distributed via messages containing links and attachments. The latter was less effective due to an extra layer of protection that prompted users to accept incoming files before any transfer could take place.

- **Botnet** – A botnet is a network of computer zombies or bots controlled by a master. Fake security notifications are the most common way to spread bots. A botnet could launch a denial-of-service attack, which cripples a server or network by sending out excessive traffic.

- **Trojan Horse** – A Trojan horse, or Trojan, is a program that appears to be legitimate but is actually malicious. Trojans might install adware, a toolbar, or a keylogger, or open a backdoor.

- **Ransomware** – Ransomware is malware that prevents you from using your computer until you pay a fee. Payment is usually requested in bitcoin, an anonymous, digital, encrypted currency.

- **Rootkit** – A rootkit is a set of programs that allows someone to gain control over a computer system while hiding the fact that the computer has been compromised. A rootkit is almost impossible to detect. It allows the machine to become further infected by masking behavior of other malware.

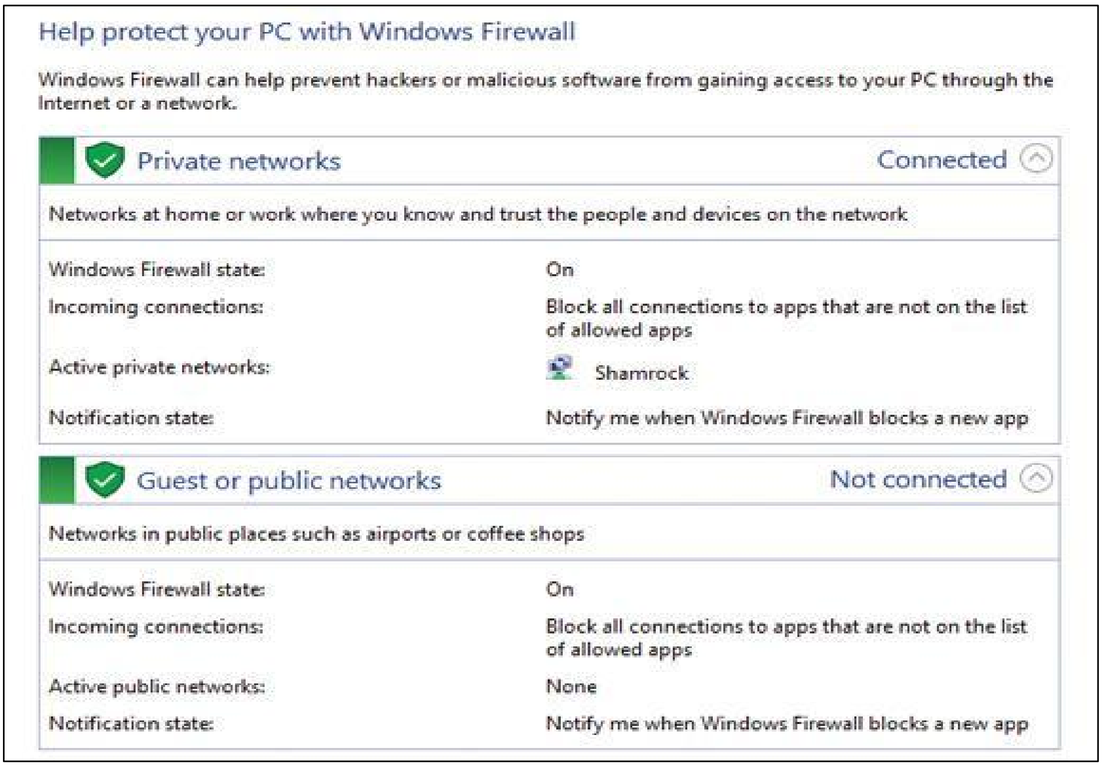
How to Secure a Computer?

One of the most common ways to get a malware infection on a computer is by downloading it. This could happen in a drive-by download. A **drive-by download** occurs when you visit a website that installs a program in the background without your knowledge.

Shields Up: Software

○ **Firewall**

- A firewall is designed to block unauthorized access to your network, but a software firewall blocks access to an individual machine.



Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	Shamrock
Notification state:	Notify me when Windows Firewall blocks a new app

Guest or public networks — Not connected

Networks in public places such as airports or coffee shops

Windows Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	None
Notification state:	Notify me when Windows Firewall blocks a new app

Figure 7. Windows Firewall

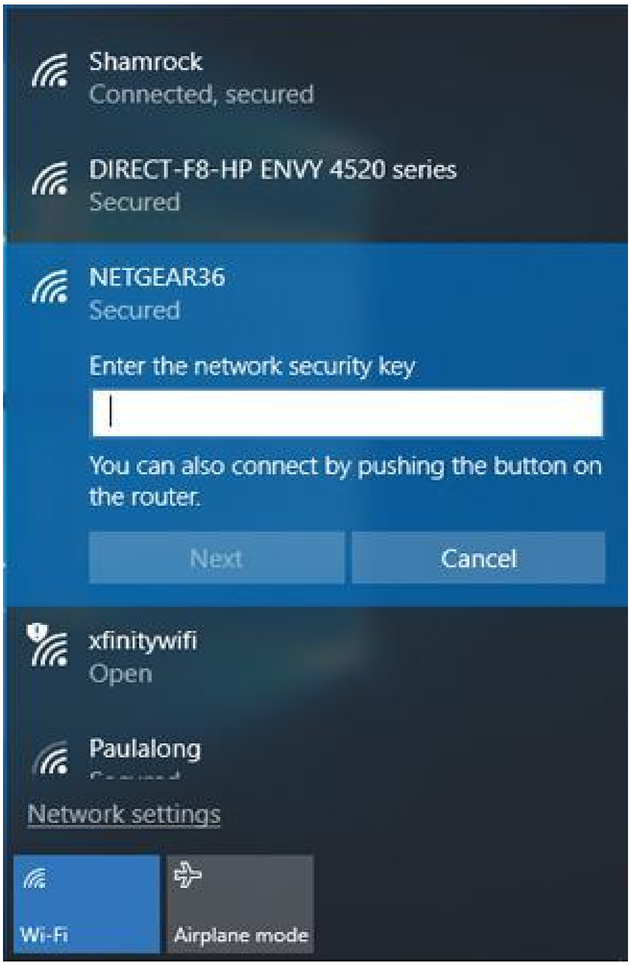
○ **Anti-virus program**

- Protects against viruses, Trojans, worms, spyware

- **Antispyware program**
  - Prevents adware and spyware from installing
- **Security suite**
  - Package of security software
  - Combination of features

Shields Up: Hardware

- **Router**
  - Connects two or more networks together
  - Home router acts like firewall
- **Network address translation (NAT)**
  - is a router security feature that shields devices on a private network (home) from the public network, Internet.
- **Wireless router –** provides a wireless access point to your network. Use the router setup utility to change the SSID, service set identifier, or wireless network name, and enable and configure wireless encryption.



Enter the network security key

You can also connect by pushing the button on the router.

Figure 7. Wireless Network by wireless router

Shields Up: Operating System

- **Update OS**
  - Keep patched and up–to–date
  - The operating system is the most important piece of security software. It is best to keep it patched and up–to–date. By default, Windows and OS X computers are configured to automatically install updates. The only way to try to be safe is to be proactive and diligent in protecting your computer system.