Computer Infections

Types of Infections

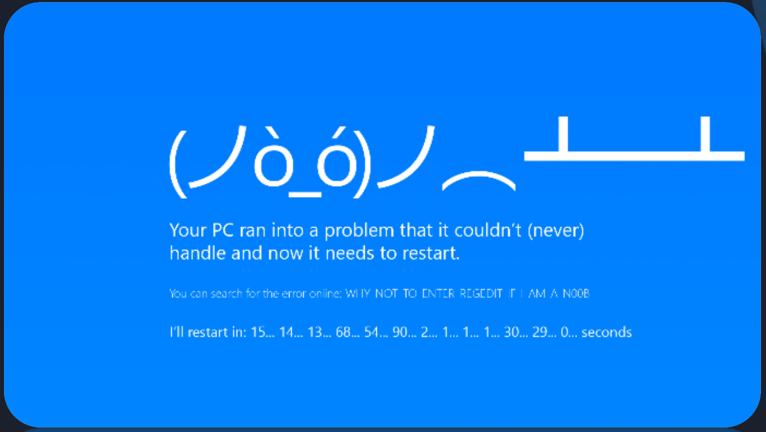
ICTSAS308

aie

SPECIALIST EDUCATORS IN
GAMES, ANIMATION & FILM VFX

Contents

- *What Could Possibly Go Wrong*?
- *Identify* different types of computer infections:
  - Spam, Scams and Fraud
  - Types of Malware
  - Viruses, Worms and Trojans
- Diagnose and Defend



(╯ò_ó)╯︵ ┻━┻

Your PC ran into a problem that it couldn't (never) handle and now it needs to restart.

You can search for the error online: WHY NOT TO ENTER REGEDIT IF I AM A N00B

I'll restart in: 15... 14... 13... 68... 54... 90... 2... 1... 1... 1... 30... 29... 0... seconds

What Could Possibly Go Wrong?

- Corporate hacking can result in:
  - Loss of information (trade secrets, customer info)
  - Loss of reputation
  - Loss of employee morale
  - Loss of business
  - Lawsuits from:
    - Shareholders
    - Business partners

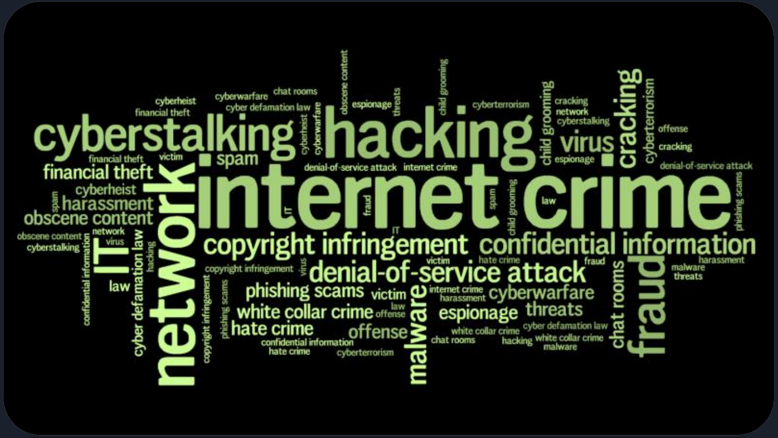
What Could Possibly Go Wrong?

- Personal consequences of hacking/online scams:
  - Loss of information
  - Information theft
  - Identity theft (e.g. Steam account)
  - Financial costs
  - Loss of productivity
    - System performance degradation
    - Deleted data
    - System corruption

How do these problems arise?

- Malicious actors can cause us damage by hacking:
  - *Guessing/cracking* passwords
  - Using *scripts*, *viruses* or *malware* to gain access

- So what are the types of threats we need to *protect a system* against?



Spam, Scams and Fraud

- Email Spam
  - The *mass distribution of unsolicited* messages, advertising or pornography to addresses which can be easily found on the Internet

- What it can do:
  - *Annoy you* with unwanted junk mail
  - *Crowds out the important email* / overflows your email account
  - *Burdens communication* service providers
  - *Phish for info* by tricking you into following links or entering details
  - *Is a vehicle* for malware, scams, fraud and threats to your privacy

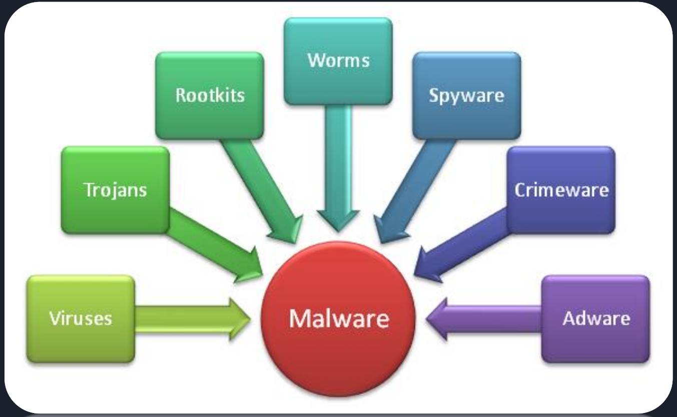
Spam, Scams and Fraud

- Phishing and Smishing Scams:
  - Phishing Emails or Smishing SMS look real
    - Like they came from a real company
  - Their goal is to trick you!
    - Visit a fake website
    - Send personal details

- What they can do:
  - *Provide access to personal information* that allows a criminal to access your accounts

Malware

- Malware is software that can *infect a computer*, such as:
  - Computer viruses,
  - Worms,
  - Trojan horses,
  - Spyware,
  - and Adware



- It's a *common method used* to infiltrate or damage your computer

What can Malware do?

- Intimidate you with scareware
  - E.g. Messages saying computer has a *security problem* or other *false information*
- Reformat a hard drive
- Alter or delete files
- Steal sensitive information
- Send emails on your behalf
- Take control of your computer and the software on it

Viruses

- Are malicious computer programs that reside on your computer
  - Often sent as an email attachment or a download link
  - Once installed, will infect your computer

- What they can do:
  - Send spam
  - Provide criminals with access to your computer
  - Scan and find personal information like *passwords*
  - Hijack your web browser
  - Disable your security settings
  - Display unwanted ads

Trojans

- A malicious program that is disguised as, or embedded within, legitimate software
  - E.g. Looks like a *real program*, but contains malicious software

- What they can do:
  - Delete your files
  - Use your computer to hack other computers
  - Watch you through your web cam
  - Log your keystrokes
  - Record usernames, passwords and other personal info

Worms

- Works on its own without attaching itself to files/programs
  - Has the capability to *spread without any human action*
  - Lives in your computer memory
  - Doesn't damage or alter the hard drive
  - Propagates by sending itself to other computers in a network

- What they can do:
  - Spread to everyone in your contact list
  - Cause tremendous damage by shutting down parts of the Internet, or wreaking havoc on an internal network

What can we do to stay protected?

- Maintain your operating systems
  - Ensures the latest security patches installed
- Install and use a virus scanner
  - Set up a schedule to automatically run full system scans
- Use different (strong) passwords for each login
  - A password manager like 1Password or LastPass can help
  - If a password is breached, other sites aren’t compromised

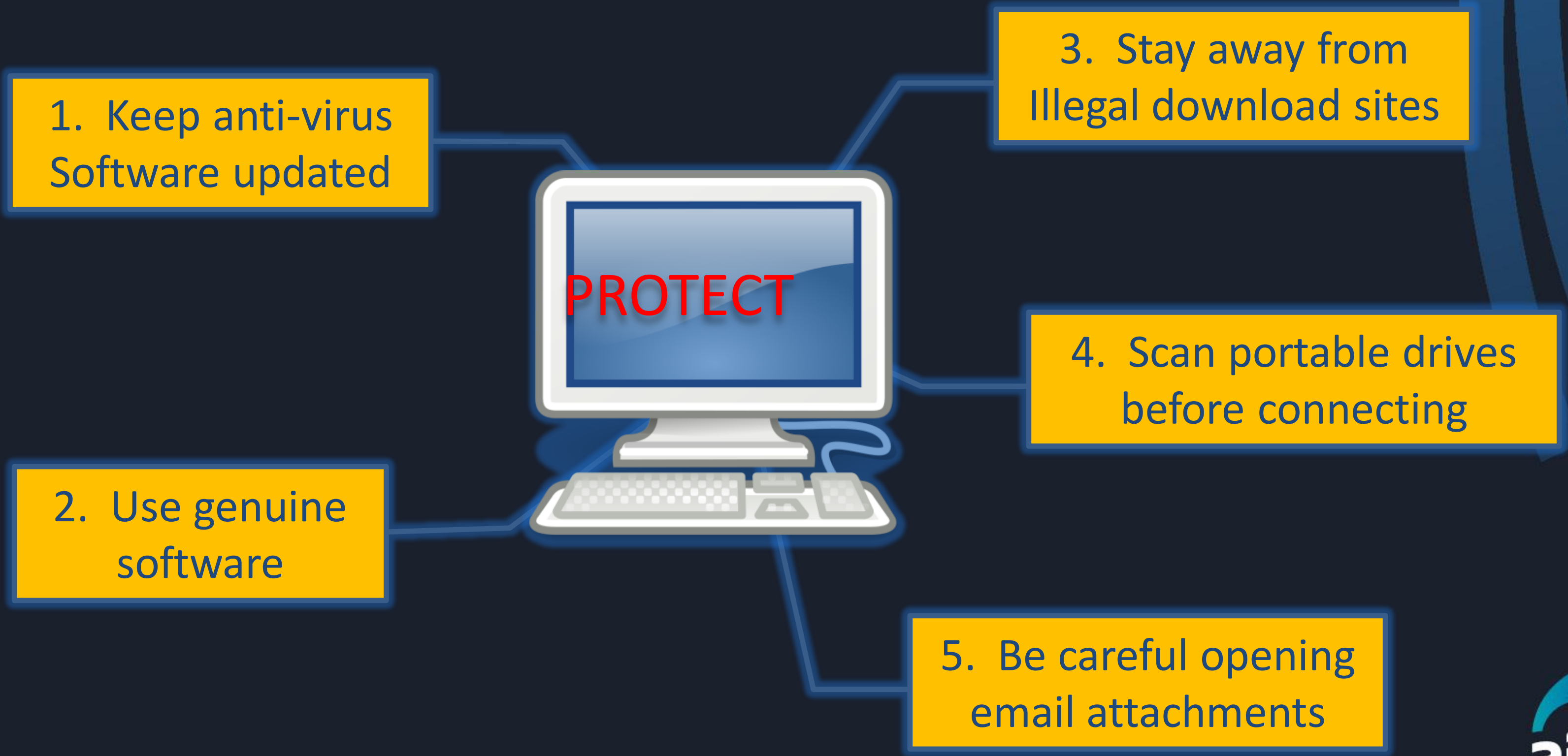
Defending against Infections

- *Enable* the security features of your OS
  - Use User Accounts
  - User Access Controls, software permissions to install or change

- Pay attention to software installers
  - Even legitimate software sometimes installs adware

- Check what you are installing
  - All software (even Open Source software) may contain Trojans

Defending against computer infections



PROTECT

1. Keep anti-virus Software updated
2. Use genuine software
3. Stay away from Illegal download sites
4. Scan portable drives before connecting
5. Be careful opening email attachments

Summary

- *Examined* problems associated with computer infections, and their impact on an organisation

- *Identified* different types of computer infections:
  - Spam, Scams and Fraud
  - Types of Malware
  - Viruses, Worms and Trojans

- *Discussed* how to *diagnose* and *defend against infections*

References

- The Huffington Post. 2016. *Why Internet Security Matters*. [ONLINE] Available at: http://www.huffingtonpost.com/william-saito/why-internet-security-mat_b_6527104.html. [Accessed 01 September 2016].

- Government of Canada. 2016. *Common Threats* . [ONLINE] Available at: http://www.getcybersafe.gc.ca/cnt/rsks/cmmn-thrts-en.aspx#s03. [Accessed 01 September 2016].