Enable your Research with Cybersecurity!

Day 1

Prepared by:
Raphaelle Gauriau
Information Security Strategic Execution Manager, University of Toronto

A few words

- Cybersecurity Operations since 2011
- Worked in different sectors (legal, energy, security consultation)
- Compliance: NERC, ISO-27001
- Two years in High Performance Computing

Tell us something about you!

Context

- **Feedback** from the researchers' community **has shown disparities** in security knowledge
- Institutions across Canada developing **Security Training & Awareness Programs, not yet available everywhere**
- Larger context of **Digital Research Alliance of Canada**
  - Security Trainings & Awareness program in progress
  - **Future: Targeted security trainings** for researchers

Audience

- To **researchers** who…
  - are using The Alliance Clusters and Cloud
  - want to learn more about cybersecurity
  - want to know **practical best practices** from an end user perspective
  - want to **better protect** their research

Agenda

Day 1

Cybersecurity Concepts

Cybersecurity Attacks

Best practices

Assignment 1

Day 2

Best practices (suite)

Cryptography Concepts

SSH keys usage

Assignment 2

Day 3

Speaker: Rachel Zand
Director, Human Research Ethics at the University of Toronto

Human Research Data

Security and Research Ethics Board

Assignment 3

To obtain credits counting towards SciNet certificates, you will need to attend two out of the three days of this workshop and submit two out of three assignments.

Assignment 1 is due before day 2 session.
Assignment 2 and/or 3 is due by October 30 2022.

Agenda – Day 1

- Cybersecurity Concepts
- Cybersecurity Attacks
- Best practices

Assignment 1

Cybersecurity Concepts

What is Cybersecurity? (1/3)

Answers from non cybersecurity practitioners:

“It aims at protecting **digital assets**”

“It prevents **hackers** from breaking into systems and **stealing data and money**’’

“It refers to **protocols** established to **defend** information data”

“The protection against the **risks** of attacks to computers by limiting **vulnerabilities**”

What is Cybersecurity? (2/3)

What is Cybersecurity? (3/3)

- **Cybersecurity:** An approach or series of steps to **prevent or manage the risk** of damage to, unauthorized use of, exploitation of, and—if needed—to restore electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity, and availability of these systems.
- **Vulnerability:** A **weakness** in a system, application, or network that is subject to exploitation or misuse.

Source: https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary

What do we do about risks?

Scenario 1:

Arbutus Cloud Team contacts you to let you know that two virtual machines (VMs) in your Cloud lab are exposed on the Internet while they should not be.

Those VMs were configured by a researcher from your group who has retired.

What do we do about risks?

Scenario 2:

You have a Windows 2003 server in your lab environment that contains a legacy application used for some important project. It cannot be upgraded at this time.

What do we do about risks?

Scenario 1:

Arbutus Cloud Team contacts you to let you know that two virtual machines (VMs) in your Cloud lab are exposed on the Internet while they should not be.

Those VMs were configured by a researcher from your group who has retired.

Scenario 2:

You have a Windows 2003 server in your lab environment that contains a legacy application used for some important project. It cannot be upgraded at this time.

Our Options:

- **Avoid/Resolve**
- **Mitigate**
- **Transfer**
- **Accept (when none of the other options are feasible; often based on a ratio cost/benefit)**

Recurring Theme

Adding → Removing

Cybersecurity

	List of domains
1	Security and Risk Management
2	Asset Security
3	Security Architecture and Engineering
4	Communications and Network Security
5	Identity and Access Management
6	Security Assessment and Testing
7	Security Operations
8	Software Development Security

Source: https://resources.infosecinstitute.com/certification/the-cissp-domains-an-overview/

Defense in-depth

Types of defense

- **Physical Controls**

  Examples: security guards; locked doors.

- **Technical Controls**

  Examples: firewalls; anti-virus.

- **Administrative Controls**

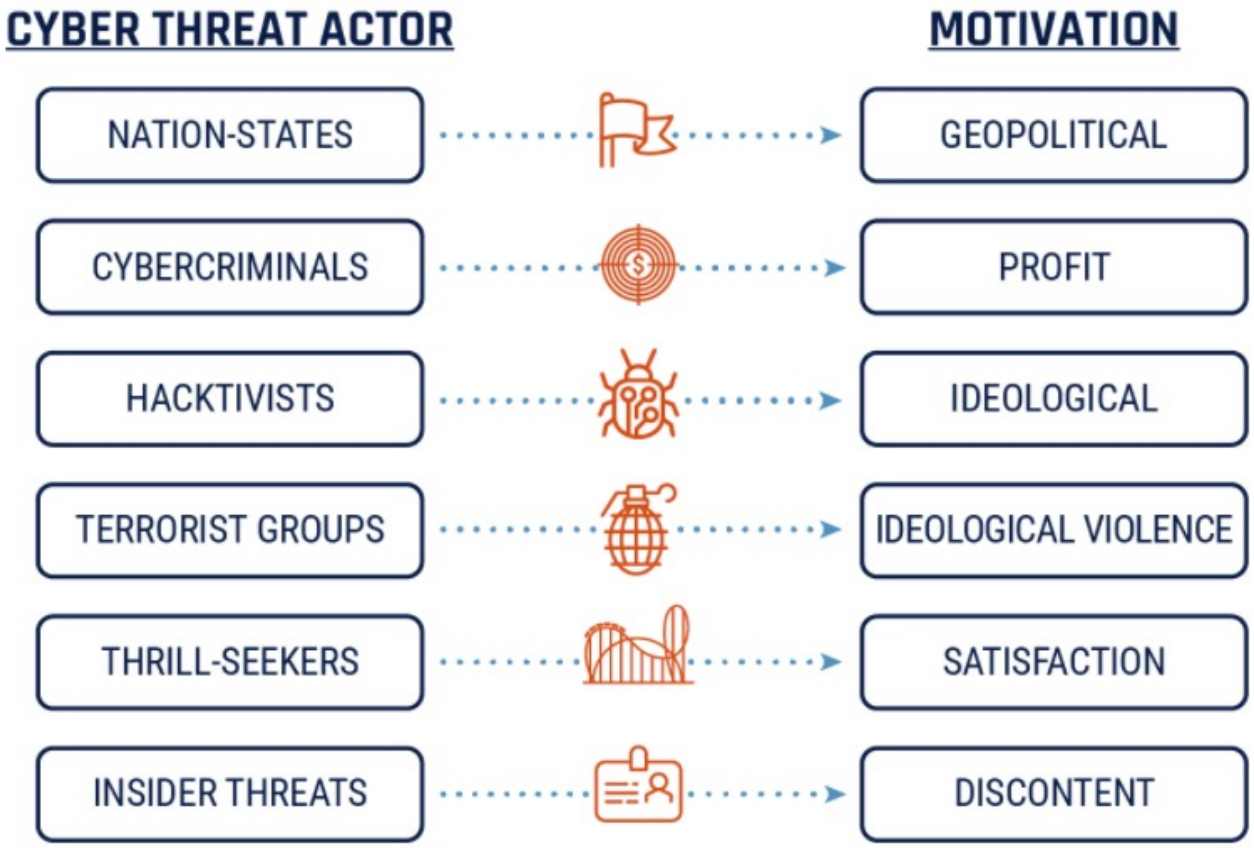
  Examples: training employees against phishing attacks.

Cybersecurity Attacks

“If you **know the enemy and know yourself**, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”

Sun Tzu, *The Art of War*

Who are the attackers?



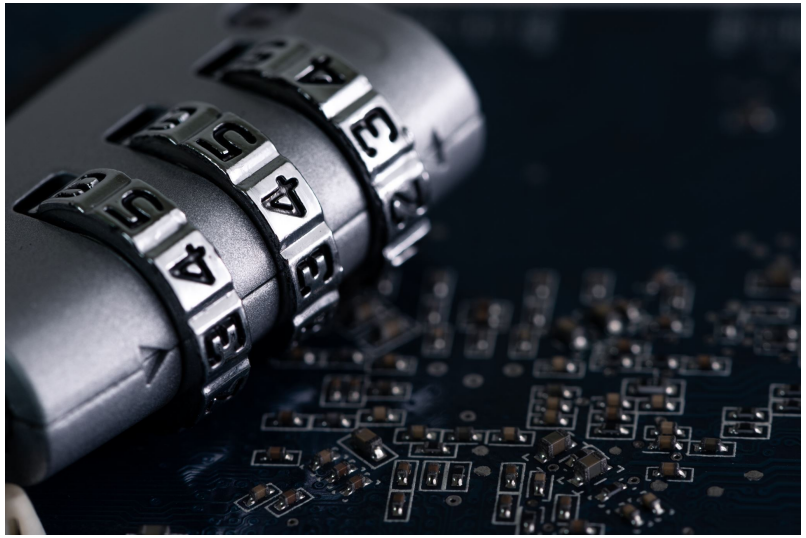
Source: https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors

Scenario – let’s be creative!

You are a white hat and have been tasked to steal the list of personal information at company X as part of a security mandate.

How do you achieve this goal?

What are the steps?

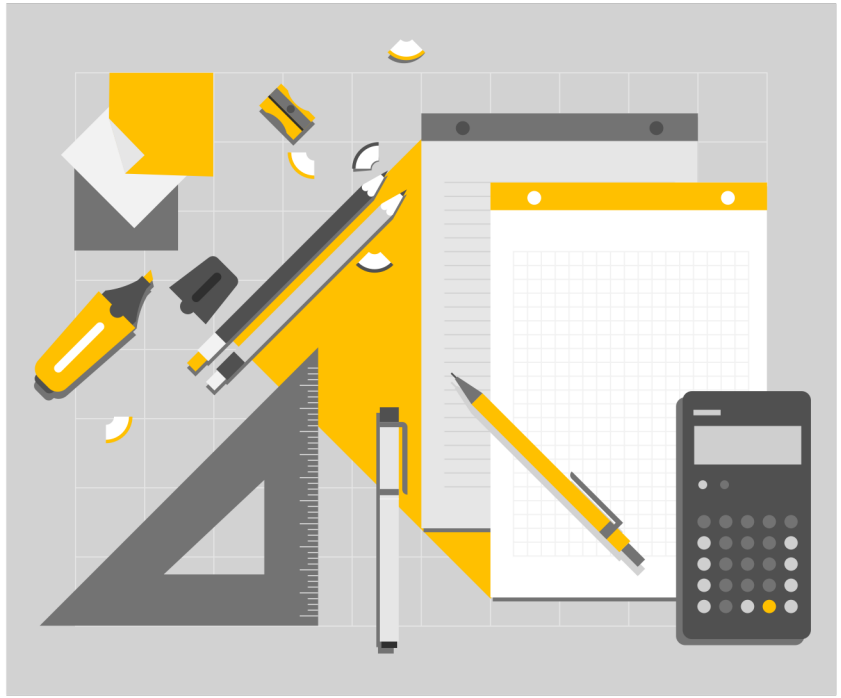


Source: PowePoint stock images

Scenario – step 1

Gather information

- Collect information on the employees
- Go to company X office, monitor trends
- Collect technical details



Source: PowerPoint stock images

Scenario – step 2

Craft the attack

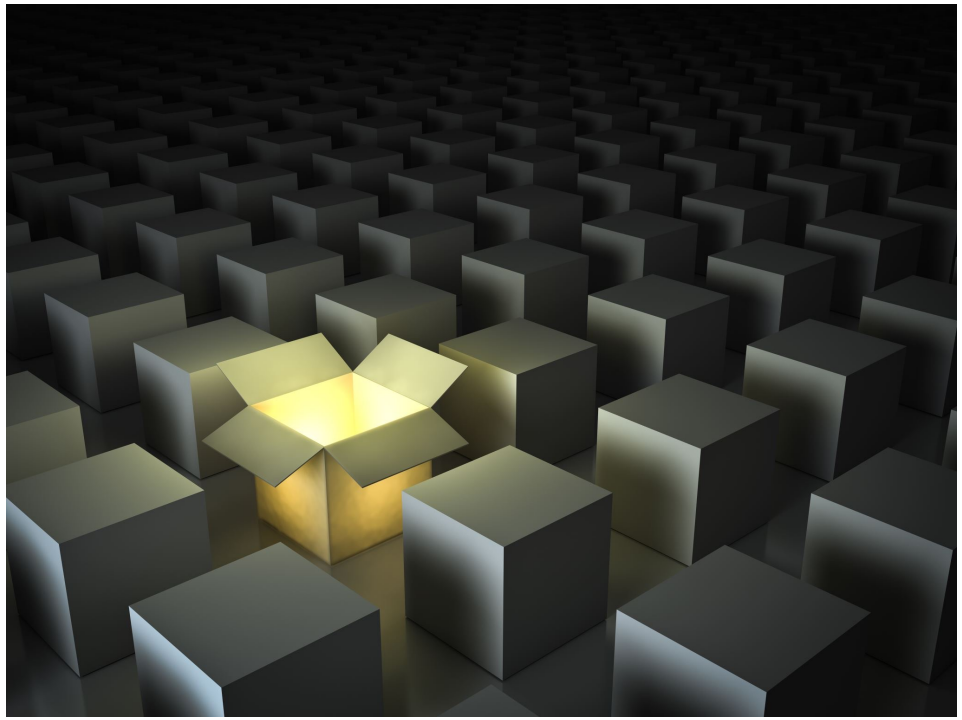
- Define initial access (phishing, external remote access, trusted relationship…)
- Payload

Source: PowerPoint stock images

Scenario – step 3

Deliver, exploit, install

- Execute the attack previously crafted
- Compromise system



Source: PowerPoint stock images

Scenario – step 4

Command&Control, Achieve objective

- Escalate privileges
- Move laterally
- Steal personal information

Source: PowerPoint stock images

Cyber Kill Chain

Anonymous Survey –

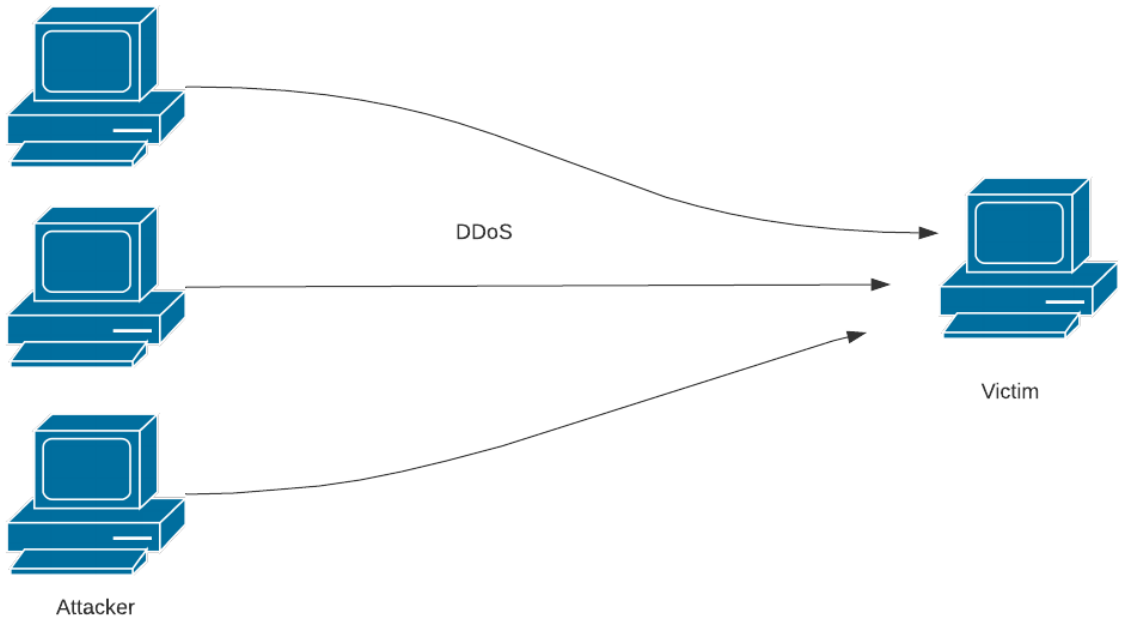
What is your workstation's operating system?

Types of Cyberattacks – Malware (1/4)

- Malicious computer program
- Many types: viruses, worms, ransomware, Trojan horses, rootkits…
- Popular: Ransomware
- How to prevent them: anti-malware; keep your systems updated

Types of Cyberattacks – DoS (2/4)

- DoS = Denial of Service
- DDoS = Distributed Denial of Service
- Makes a machine or network resource unavailable
- How to prevent them: Intrusion Prevention System (IPS)



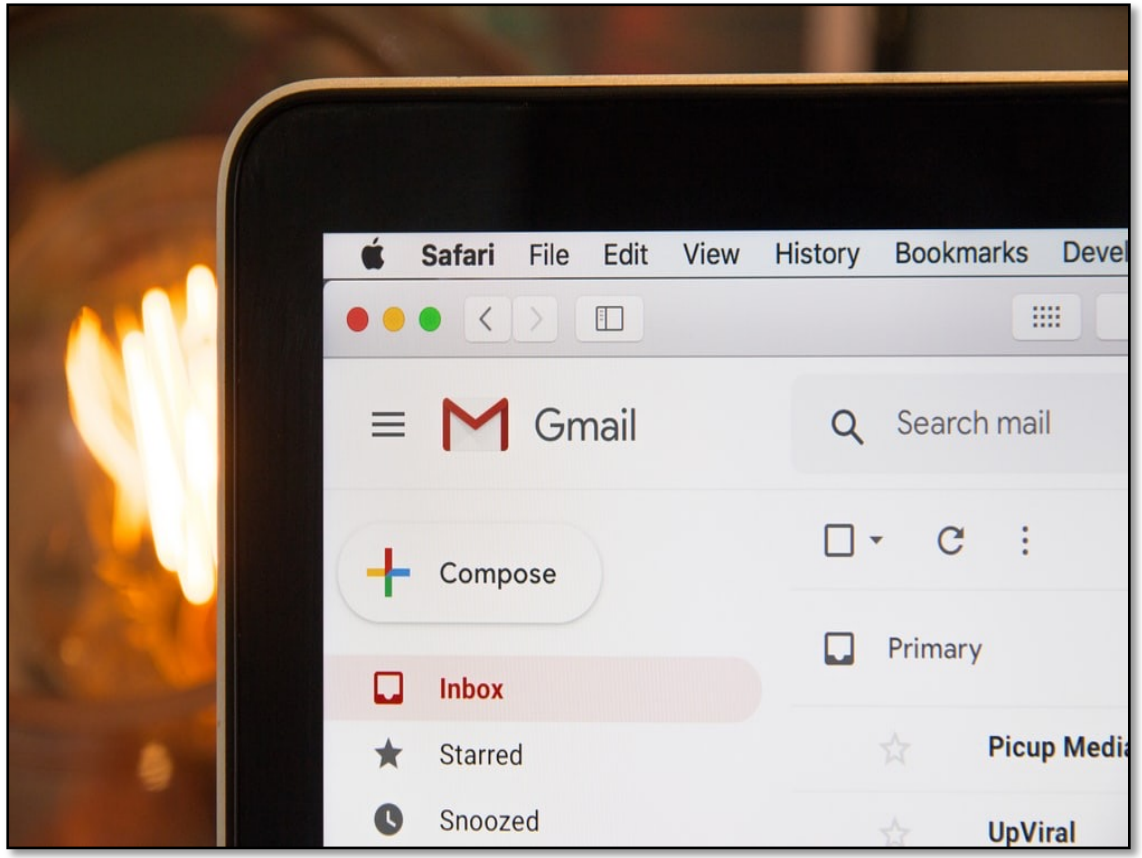
Types of Cyberattacks – Man-in-the-Middle (3/4)

- Proxies the data between the sender and recipient

- How to prevent it: encryption

Types of Cyberattacks - Phishing (4/4)

- Attempts to acquire sensitive data
- Emotions
- Increase during the pandemic
- How to prevent them: users training awareness



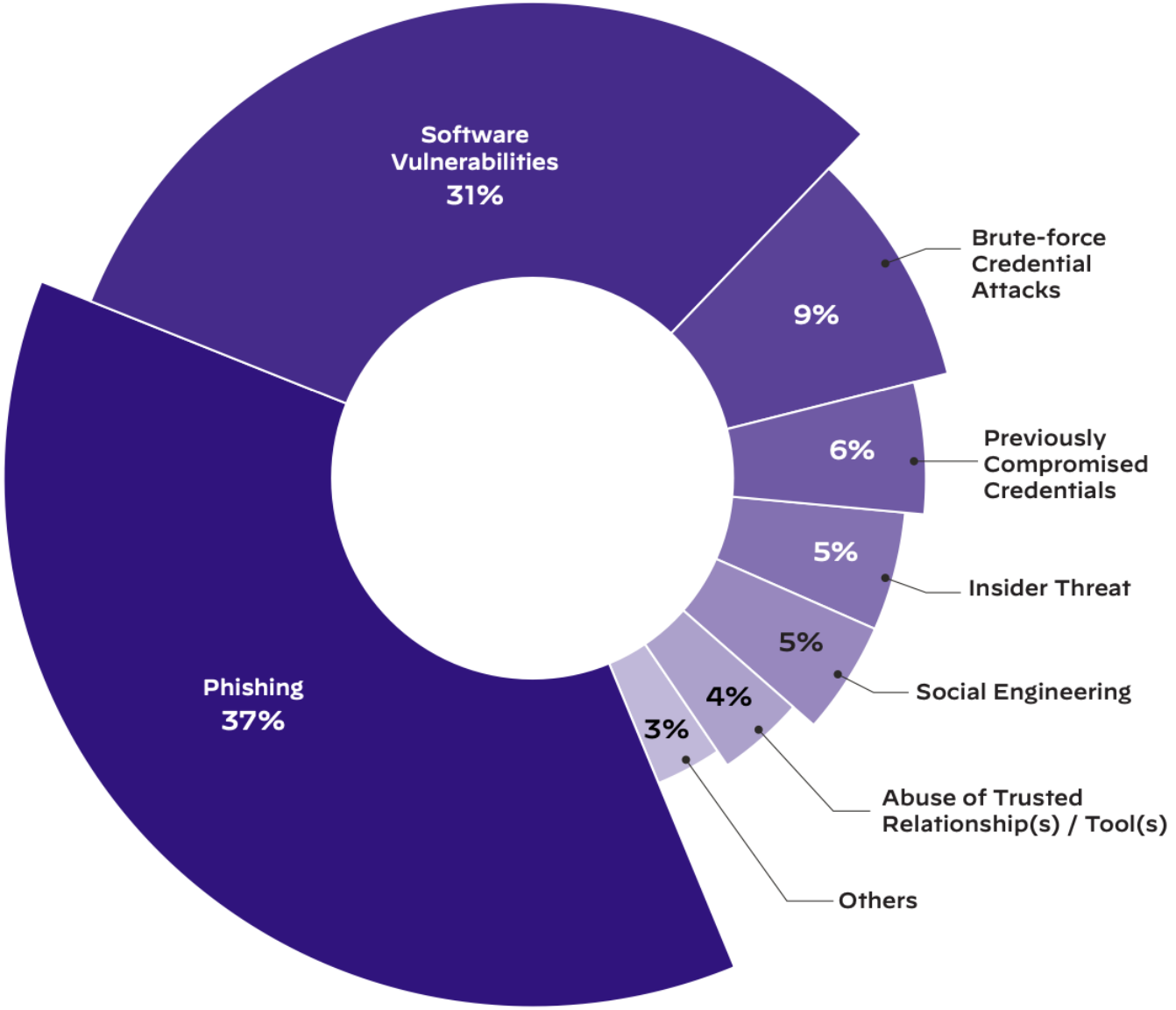
Individual vs Behavior

- Distinguish the person from their behaviors
- A lot can be prevented by **changing our own behaviors**
- **Don’t try to change everything at once, pick one thing!**
- **No blaming**

Best Practices

End-Users

What attackers are going after in 2022



Suspected Means of Initial Access

Source: Palo Alto Unit 42 Incident Response Report 2022

Anonymous Survey –

How often do you patch (update) your workstation?

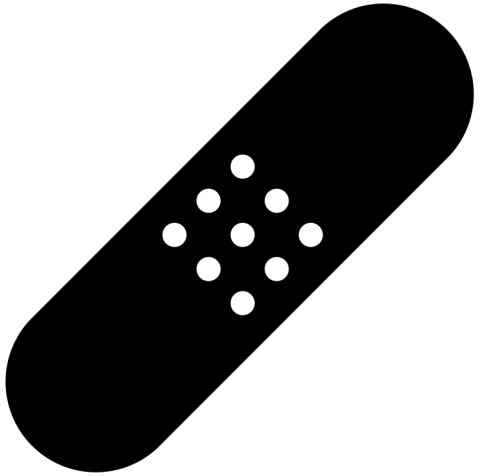
Do I really need to patch (update)?

But… I am using multi-factor authentication!

But… I am using a VPN!

But… I am only browsing on websites I know!

YES – YOU STILL NEED TO PATCH.



WannaCry

- Happened in **May 2017**
- **Ransomware** infected over **230,000 machines** in over **150 countries**
- Estimated: **$4 billion in losses** across the globe.
- Organizations impacted: Telefónica (Spain); thousands of NHS hospitals and surgeries (UK); Fedex (US); Universities (China) etc….
- **Spreads itself** within corporate networks **without user interaction**

Source: https://www.sentinelone.com/blog/are-we-done-with-wannacry/
https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

WannaCry

- **U.S. National Security Agency** discovered a vulnerability in Windows protocol SMBv1 and **developed a code** to exploit it, called **EternalBlue**
- **Shadow Brokers** hacking group **stole the code** and made it public before WannaCry hit
- Patch released in **March 2017**: MS17-010

Source: https://www.sentinelone.com/blog/are-we-done-with-wannacry/
https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

Cyber Kill Chain

Best practice #1 - Patch (update)

- Most breaches could be avoided by patching
- Operating systems
  - Windows, MacOS, Linux…
    - Windows 11
    - MacOS Monterey
    - Ubuntu 22.10
- Applications
  - Update to the latest version…
  - ….or uninstall them!

macOS	Latest version
macOS Monterey	12.6
macOS Big Sur	11.4
macOS Catalina	10.15.7
macOS Mojave	10.14.6
macOS High Sierra	10.13.6
macOS Sierra	10.12.6
OS X El Capitan	10.11.6
OS X Yosemite	10.10.5

Exercise 1

Take a moment to collect the following information:

- Check your operating system version
- Find some application that needs to be updated or that is not needed anymore

Best practice #2 - Be careful of phishing

- One of the most popular vector of attack

- Indicators of phishing:
  1. An Unfamiliar Tone or Greeting
  2. Grammar and Spelling Errors
  3. Inconsistencies in Email Addresses, Links & Domain Names
  4. Threats or a Sense of Urgency
  5. Suspicious Attachments

- In doubt: contact the sender via other means, or ask your home institution's security team

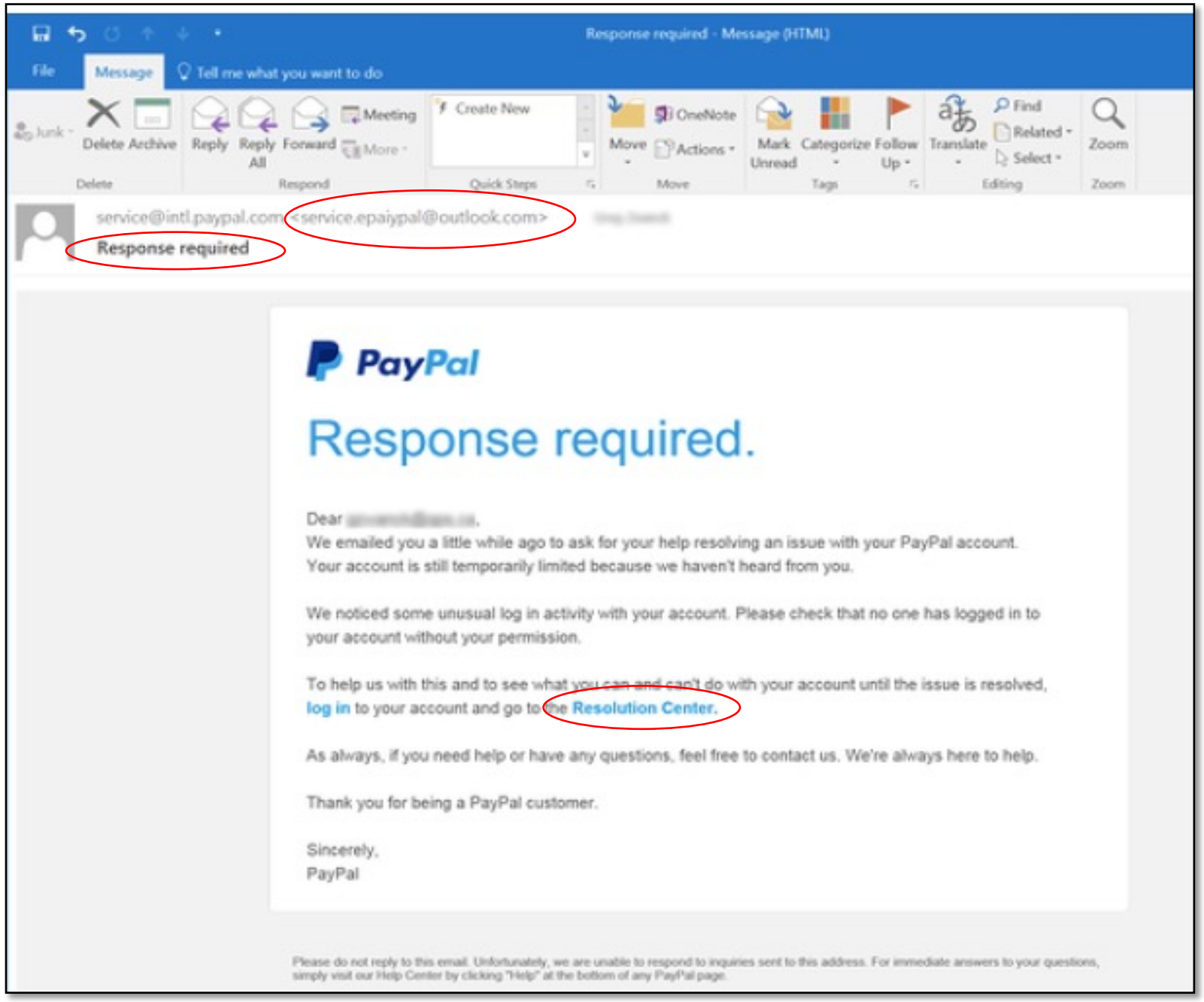
Sources: https://cofense.com/knowledge-center/signs-of-a-phishing-email/
https://www.pexels.com/photo/man-in-red-shirt-wearing-black-framed-eyeglasses-3965246/

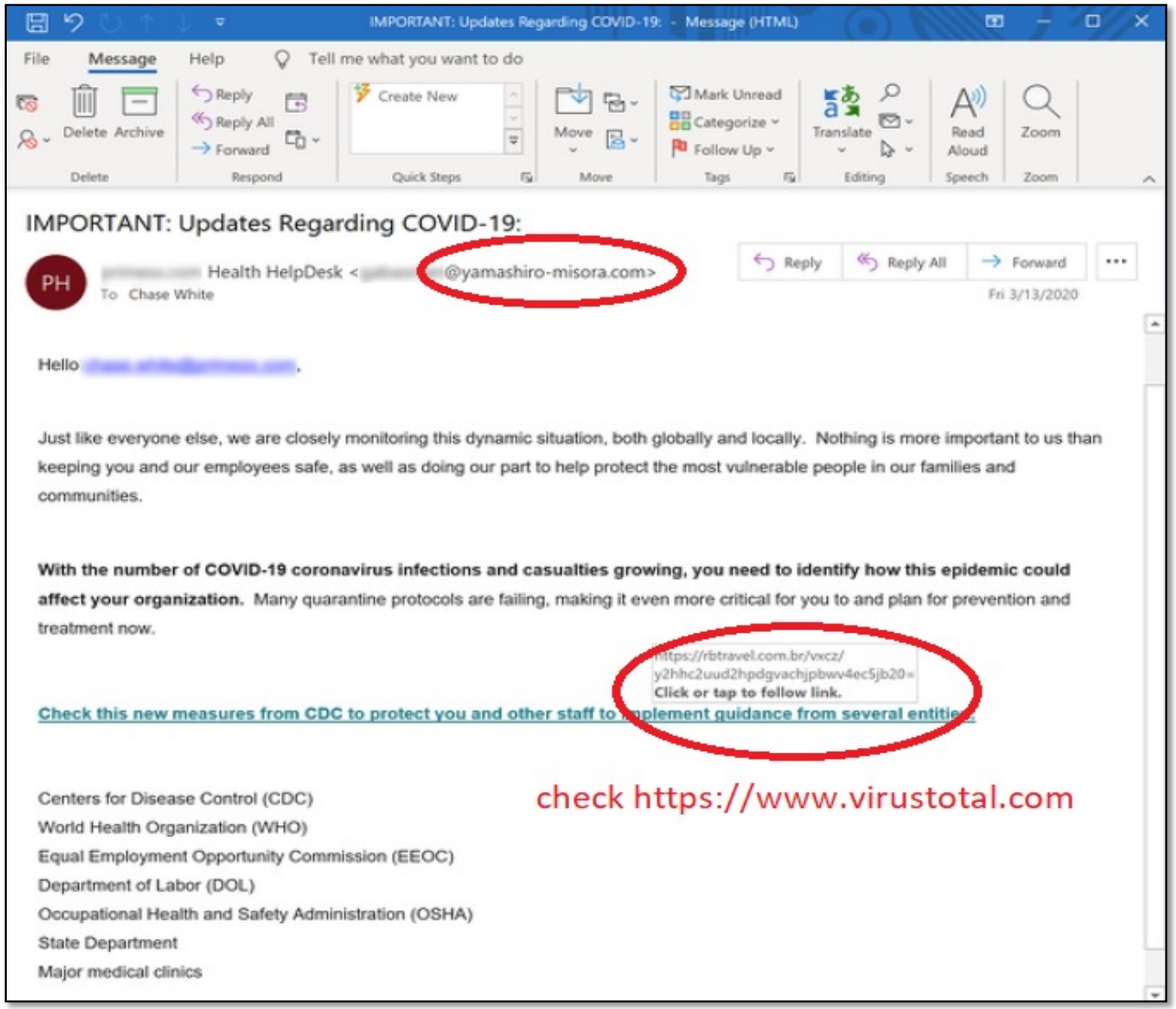
From: Dr. Jane Doe <Jane.Doe.utoronto.ca@gmail.com>
Sent on: Friday, April 10, 2020 5:58:02 PM
To: [redacted]@mail.utoronto.ca
Subject: Got a moment

Available?
--

Dr. Jane Doe
University Professor
B.Eng., M.Eng (McGill), Ph.D. (Stanford), P.Eng.
Canada Research Chair in in Transnational Molecular Geometry

Source: https://securitymatters.utoronto.ca/phish-got-a-moment/


Response required - Message (HTML)
File
Message
Tell me what you want to do
Junk
Delete
Archive
Reply
Reply All
Forward
Meeting
More
Create New
Move
OneNote
Actions
Mark Unread
Categorize
Follow Up
Translate
Find
Related
Select
Zoom
Delete
Respond
Quick Steps
Move
Tags
Editing
Zoom
service@intl.paypal.com <service.epaiypal@outlook.com>
Response required
PayPal
Response required.
Dear
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.


IMPORTANT: Updates Regarding COVID-19: - Message (HTML)
File
Message
Help
Tell me what you want to do
Delete
Archive
Reply
Reply All
Forward
Create New
Move
Mark Unread
Categorize
Follow Up
Translate
Read Aloud
Zoom
Delete
Respond
Quick Steps
Move
Tags
Editing
Speech
Zoom
IMPORTANT: Updates Regarding COVID-19:
PH
Health HelpDesk <
@yamashiro-misora.com>
To Chase White
Reply
Reply All
Forward
Fri 3/13/2020
Hello
.
Just like everyone else, we are closely monitoring this dynamic situation, both globally and locally. Nothing is more important to us than keeping you and our employees safe, as well as doing our part to help protect the most vulnerable people in our families and communities.
With the number of COVID-19 coronavirus infections and casualties growing, you need to identify how this epidemic could affect your organization. Many quarantine protocols are failing, making it even more critical for you to and plan for prevention and treatment now.
https://rbtravel.com.br/vxcz/
y2hhc2uud2hpdgvachjpbwv4ec5jb20=
Click or tap to follow link.
Check this new measures from CDC to protect you and other staff to
plement guidance from several entities
check https://www.virustotal.com
Centers for Disease Control (CDC)
World Health Organization (WHO)
Equal Employment Opportunity Commission (EEOC)
Department of Labor (DOL)
Occupational Health and Safety Administration (OSHA)
State Department
Major medical clinics

Anonymous Survey –

Do you use an antivirus on your workstation?

Types of Antivirus

Traditional methods	Modern methods
Malware signature Signature: a continuous sequence of bytes that is common for a certain malware sample. It tracks known threats	**Behavior analysis** (includes Machine learning) It detects more sophisticated attacks: unknown threats; ‘’fileless attacks’’
Heuristic analysis: detect viruses by examining code for suspicious properties - Static - Dynamic	

Source: https://www.forcepoint.com/cyber-edu/heuristic-analysis

Best practice #3 - Antivirus (1/3)

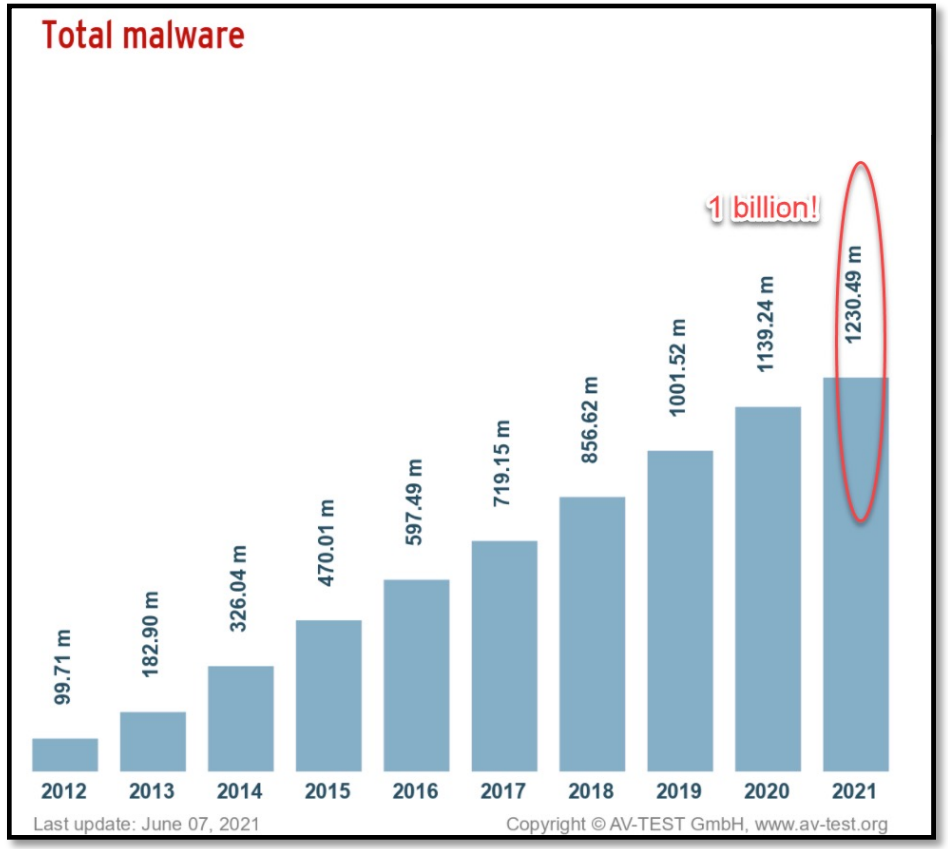
- Is it efficient?
- Do I need it for MacOS?

Trojan Flashback - Malware Top 10 for macOS

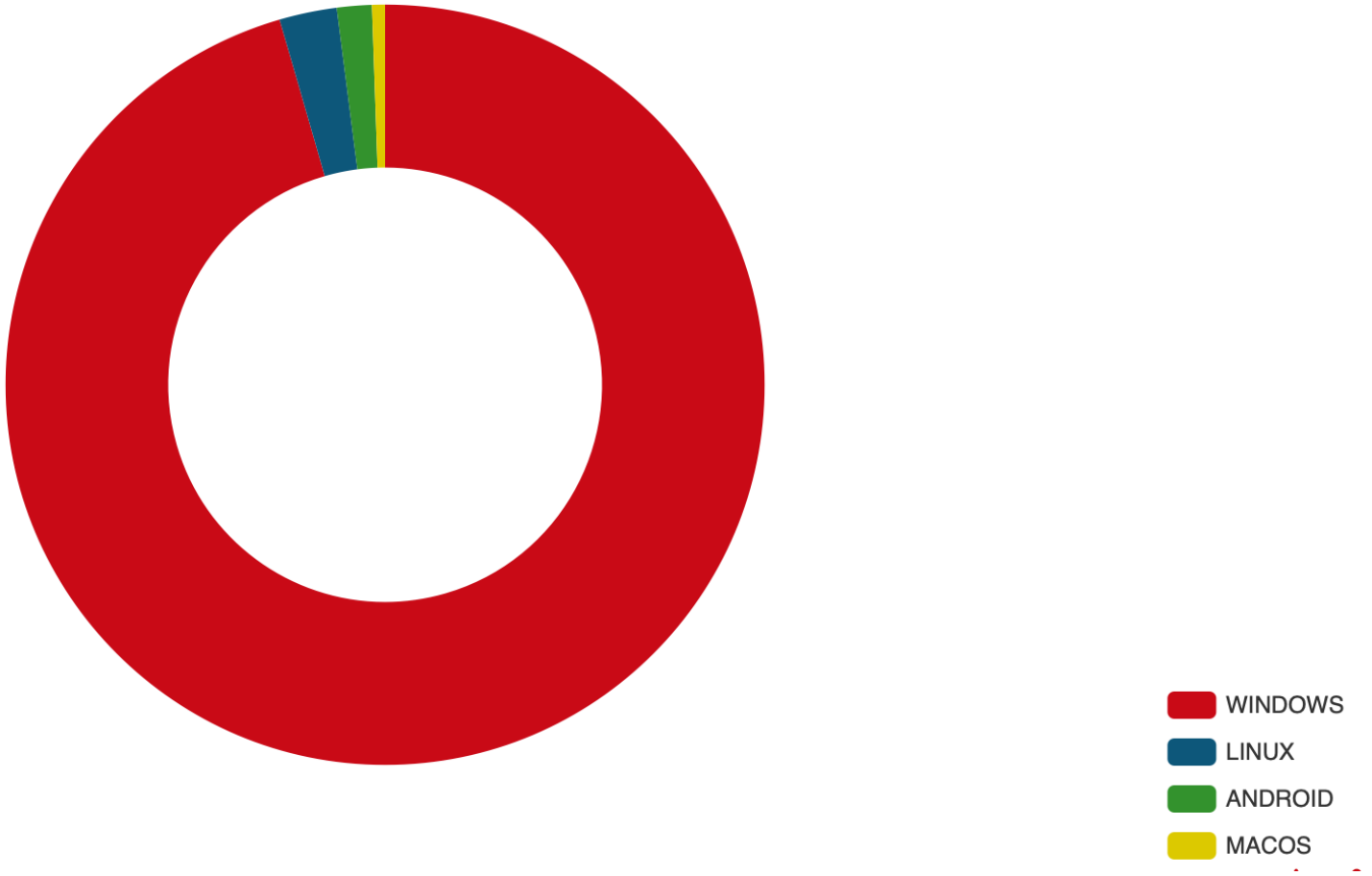
- Do I need it for Linux?

Mirai (IoT top 1)
EvilGnome spyware (2019)

- Do I need it on my mobile phone?

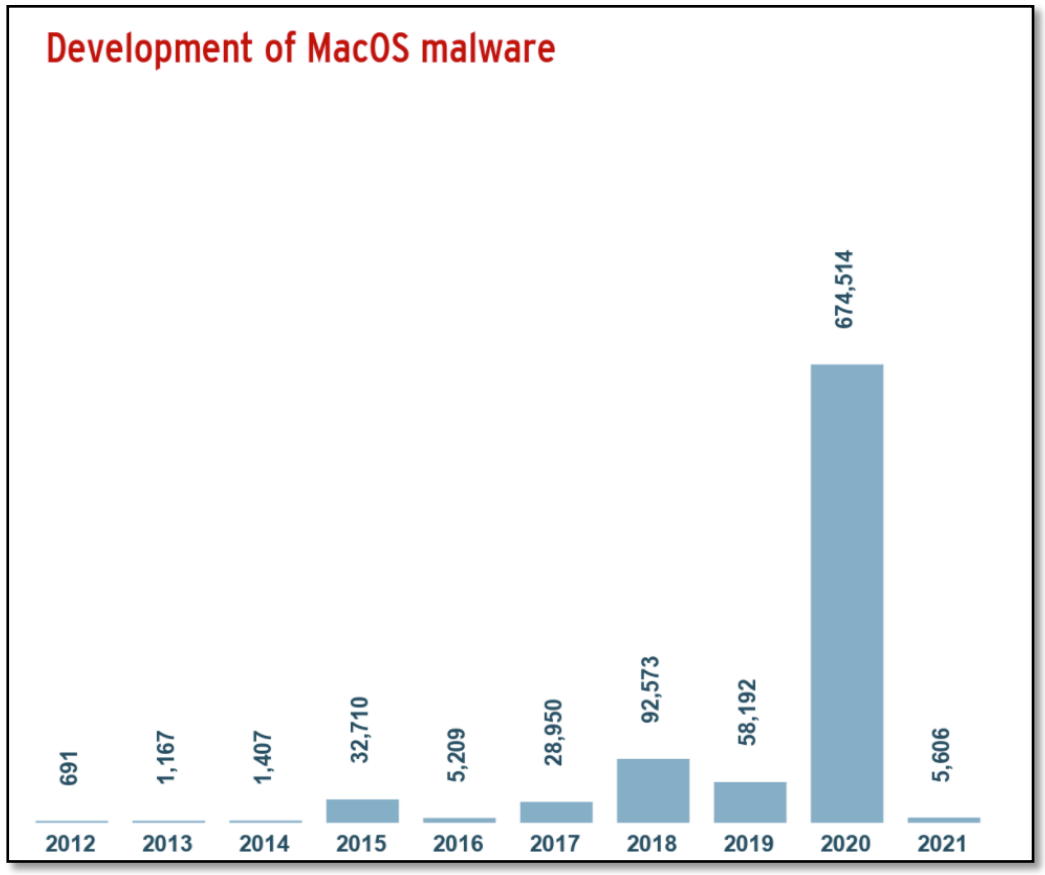


Source: AVTest Security Report 2021



Distribution of malware and PUA by operating system collected by AVTest in 2022

Best practice #3 - Antivirus (3/3)



Source: AVTest Security Report June 2021

36% of security incidents conducted by Palo Alto Unit 42 in 2022 were **Ransomware**!

Key Take-Aways – Day 1

- CIA triad
- Defense in-depth
- Keep your systems up to date!
- Be mindful of **phishing!**

Pick one thing to change!

Assignment – Day 1

1. What did you learn in today's session (1-2 items)?
2. Find one vulnerability in your workstation and remediate it (either at the operating system level or the application level).
   Note: if you are upgrading to a major version of the OS, make sure you backup your important data before proceeding.
3. Install a shell terminal with an SSH client in your computer:

   If you have a Windows workstation: install MobaXterm

   https://mobaxterm.mobatek.net/download.html

   If you have a Linux or MacOS workstation, make sure you can find the terminal.

Notes: Please write a brief report including your answers and submit them in the Education website.
For question #2, please include a few sentences describing how you found the vulnerability and how you fixed it.
For question #3, please explain what OS you are using and which application you will be using as an SSH client.

Sources and Images (day 1 and day 2)

- https://resources.infosecinstitute.com/certification/the-cissp-domains-an-overview/
- https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors
- https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary
- https://www.avast.com/en-ca/business/resources/defence-in-depth
- https://securitymatters.utoronto.ca/resources/it-professionals/ - (image)
- https://securitymatters.utoronto.ca/phish-got-a-moment/
- https://unsplash.com/s/photos/email - (image)
- https://unsplash.com/s/photos/castle - (image)
- https://www.sentinelone.com/blog/are-we-done-with-wannacry/
- https://www.kaspersky.com/resource-center/threats/ransomware-wannacry
- Palo Alto Unit 42 Incident Response Report 2022
- https://cofense.com/knowledge-center/signs-of-a-phishing-email/
- https://www.pexels.com/photo/man-in-red-shirt-wearing-black-framed-eyeglasses-3965246 – (image)
- https://www.av-test.org/en/
- https://www.forcepoint.com/cyber-edu/heuristic-analysis
- https://www.zdnet.com/article/flashback-trojan-wake-up-call-for-mac-users/
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf
- CISSP: Certified Information Systems Security Professional Study Guide, 6th Edition by Darril Gibson; James M. Stewart; Mike Chapple ; Backups Chapter
- https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
- https://www.ssh.com/academy/ssh/protocol
- https://docs.alliancecan.ca/wiki/SSH_Keys

Thank You!
Questions?