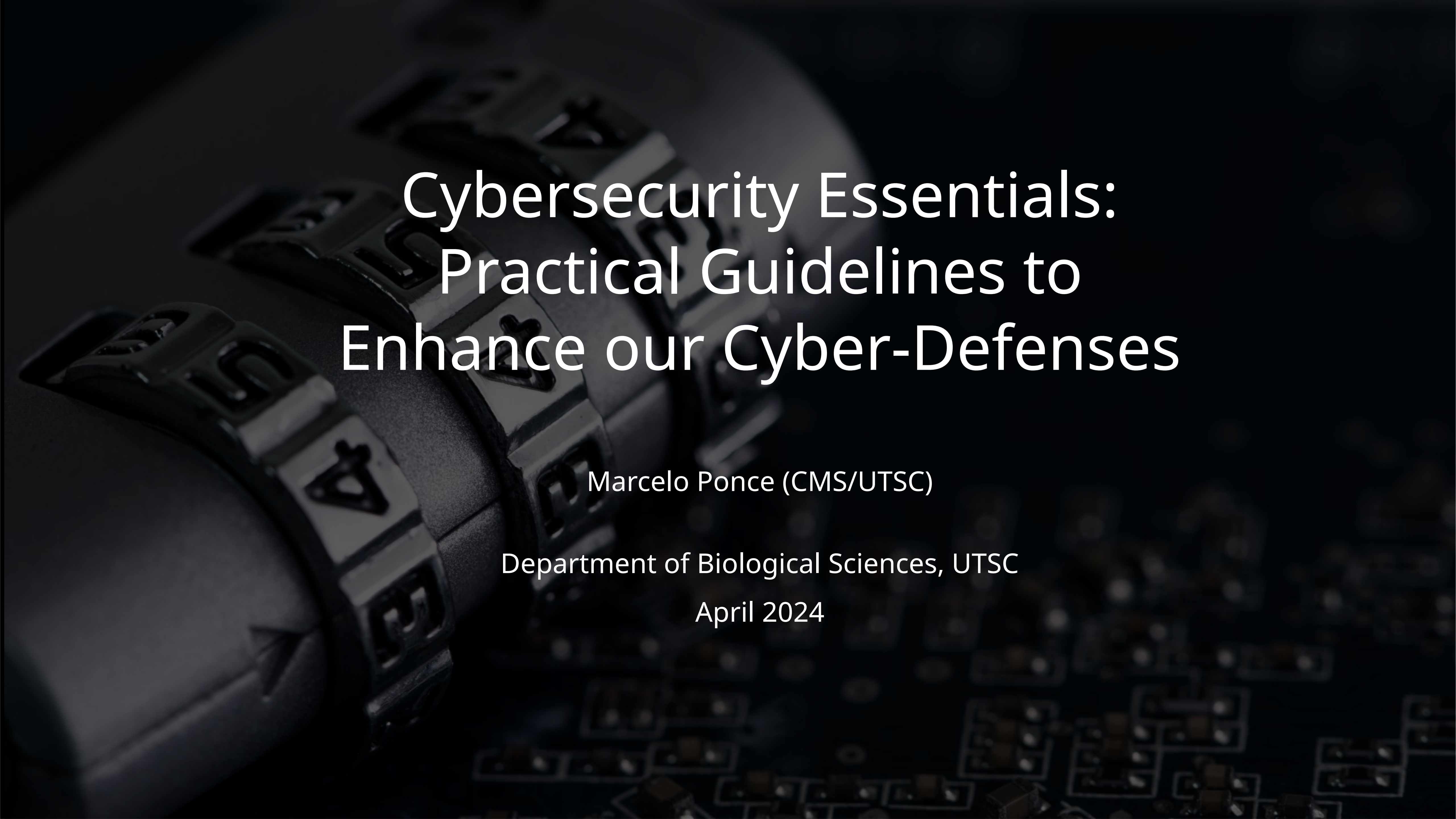


Cybersecurity Essentials: Practical Guidelines to Enhance our Cyber-Defenses

Marcelo Ponce (CMS/UTSC)

Department of Biological Sciences, UTSC

April 2024

Topics

- Cybersecurity Basics
  - Threats, Risks and Vulnerabilities, Types of Attacks
- Protecting Our Devices and Data
  - Password Hygiene, Software Updates
  - Safe Browsing Practices
- Recognizing Common Threats
  - Phishing Awareness: Identifying Suspicious Emails
  - Malware Defense: Detecting and Preventing Malicious Software
  - Social Engineering: Staying Alert to Manipulative Tactics
- Securing Our Networks
  - Firewalls and Antivirus
  - Wi-Fi Security: Protecting Your Home Network

- Securing Our Networks
  - Firewalls and Antivirus: Setting Up Basic Defenses
  - Wi-Fi Security: Protecting Your Home Network
- Data Privacy and Confidentiality
  - Encryption Basics: Safeguarding Sensitive Information
  - Data Backups: Ensuring Data Resilience
- Security Awareness Training
  - Educating End-Users: Promoting Cybersecurity Best Practices
  - Creating a Security Culture: Involving Everyone
- Legal Considerations
  - Compliance with Regulations: Understanding Data Protection Laws
  - Reporting Breaches: Legal Obligations

Cybersecurity Basics

Cybersecurity: *myths* and reality

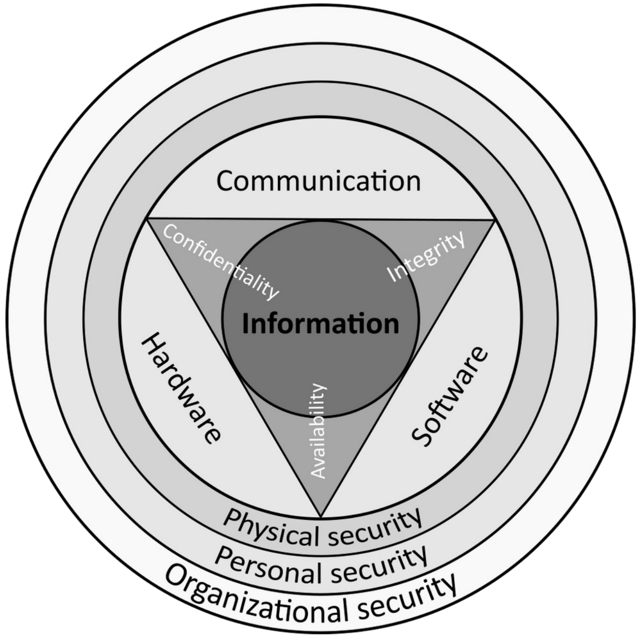
- Cybersecurity Is Solely IT’s Responsibility.
- Cyber security is *too complex* for me to understand.
- Cyber-attacks are *sophisticated*. We can’t stop them.
- Cyber-attacks are *highly targeted*.
  Our organization is unlikely to be interesting and/or valuable enough to attackers.
- More secure postures come at the expense of *more complex approaches*.

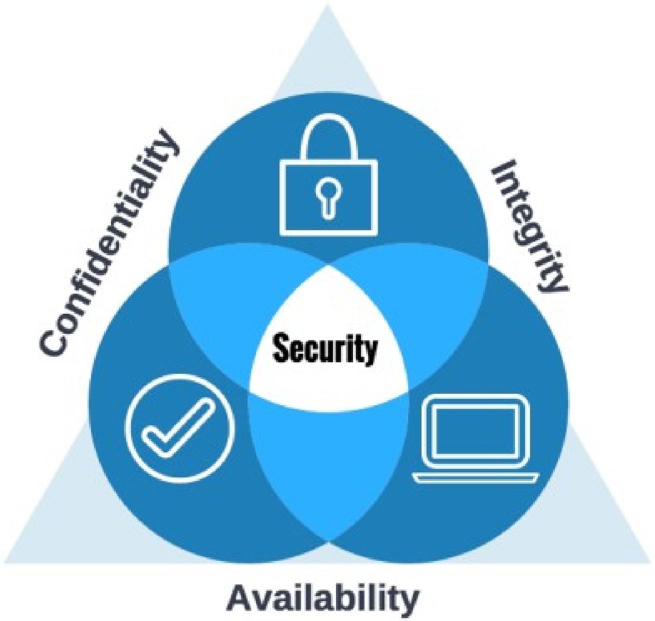
What is Cybersecurity?

- **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

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





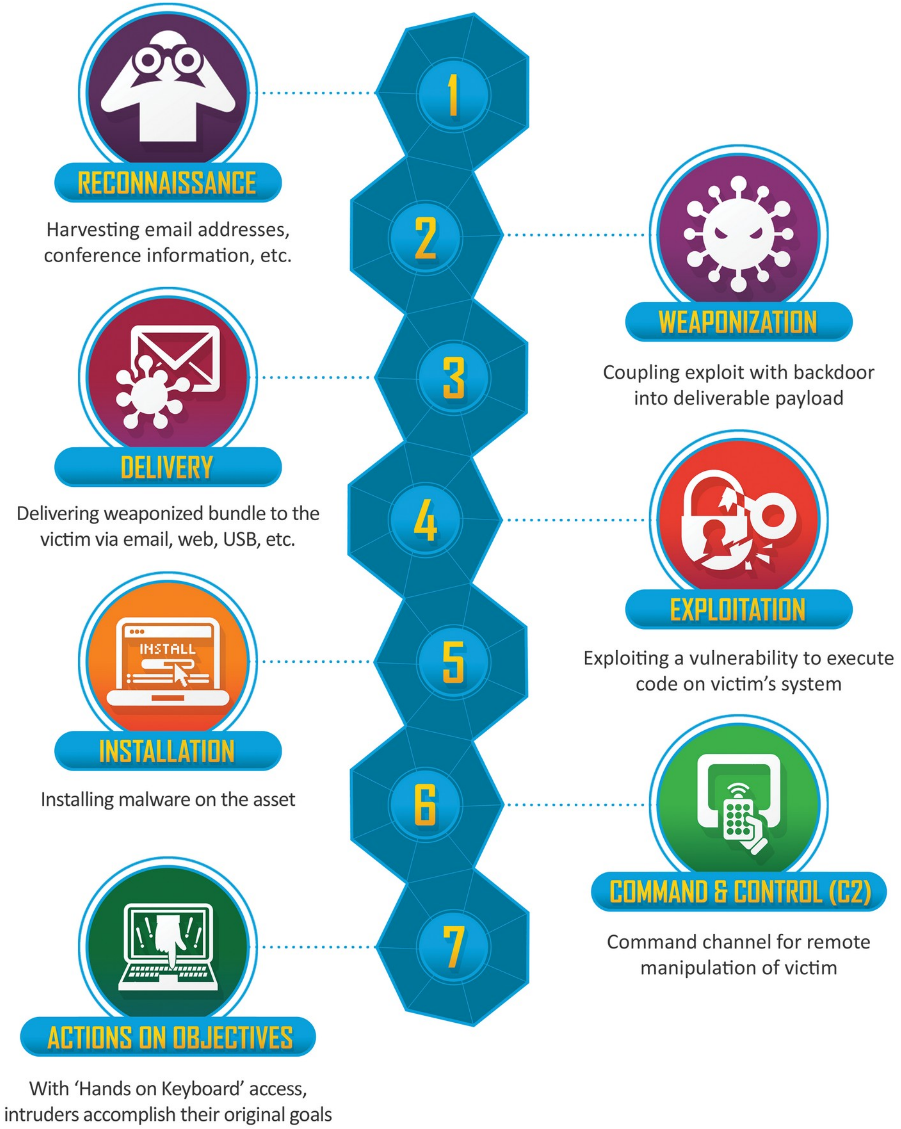
NIST CIA Triad

Types of CyberAttacks

Malicious computer program - Malware

- *Many types*: viruses, worms, ransomware, Trojan horses, spyware, rootkits
  - Popular: Ransomware
- How to prevent them:
  - *Anti-malware, anti-viruses*
  - keep our systems ***updated***

https://thevarsity.ca/2024/01/15/data-from-u-of-t-students-threatened-by-moveit-ransomware-attack/



1 RECONNAISSANCE
Harvesting email addresses, conference information, etc.

2 WEAPONIZATION
Coupling exploit with backdoor into deliverable payload

3 DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.

4 EXPLOITATION
Exploiting a vulnerability to execute code on victim's system

5 INSTALLATION
Installing malware on the asset

6 COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim

7 ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Cyber Kill Chain (src: Lockheed Martin)

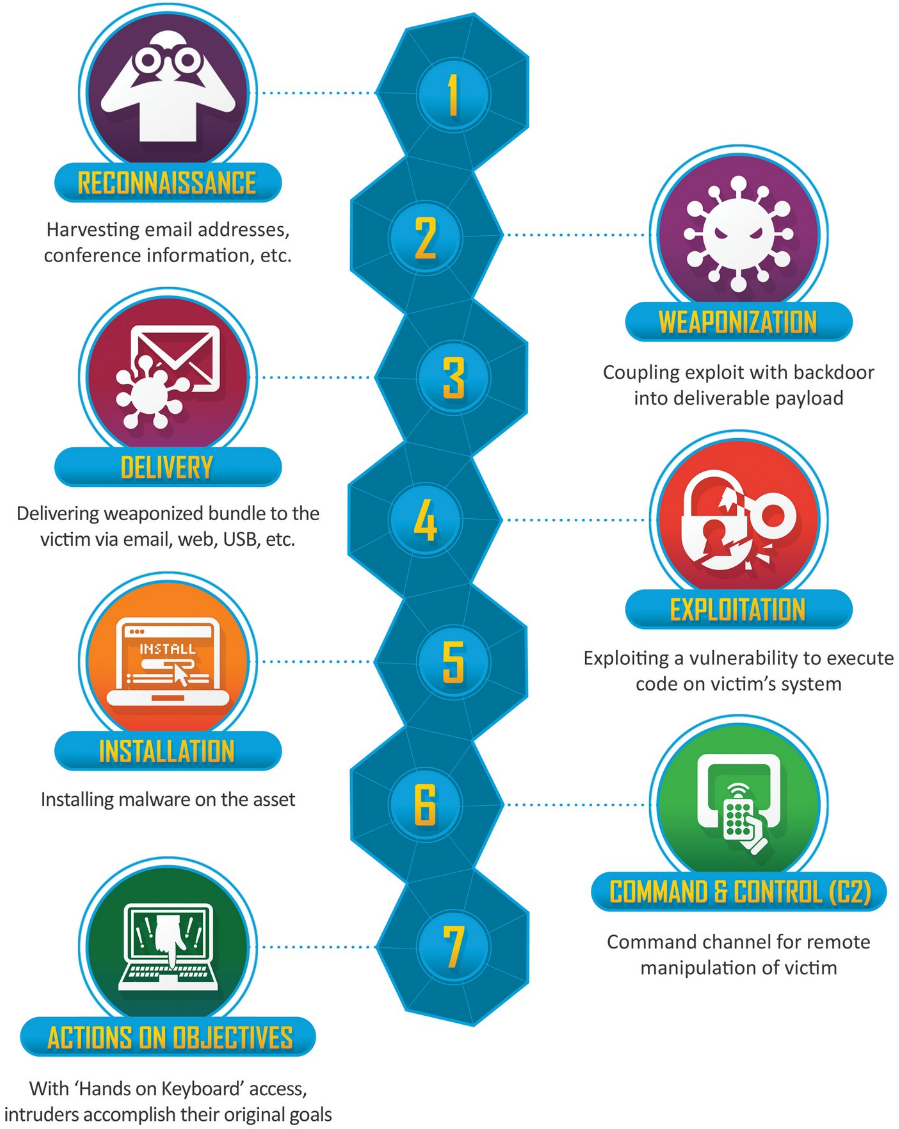
Types of CyberAttacks

Phishing

- Deceptive emails or messages aiming to steal sensitive information.
  - Appeal to “emotions”
- How to prevent them:
  - *Training and education*
  - *Cybersecurity Awareness*

- Malitious QR codes: *quishing*

Ref. https://securitymatters.utoronto.ca/quishing-on-the-rise/


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim’s system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With ‘Hands on Keyboard’ access, intruders accomplish their original goals

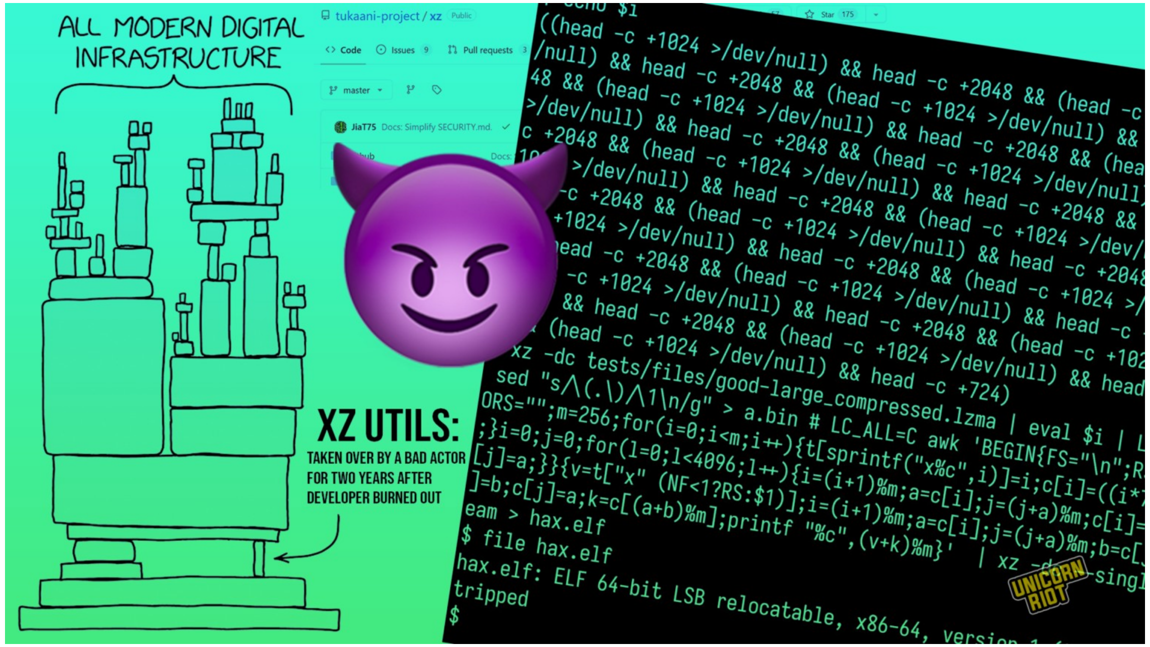
Cyber Kill Chain (src: Lockheed Martin)

Types of CyberAttacks – *Social Engineering*

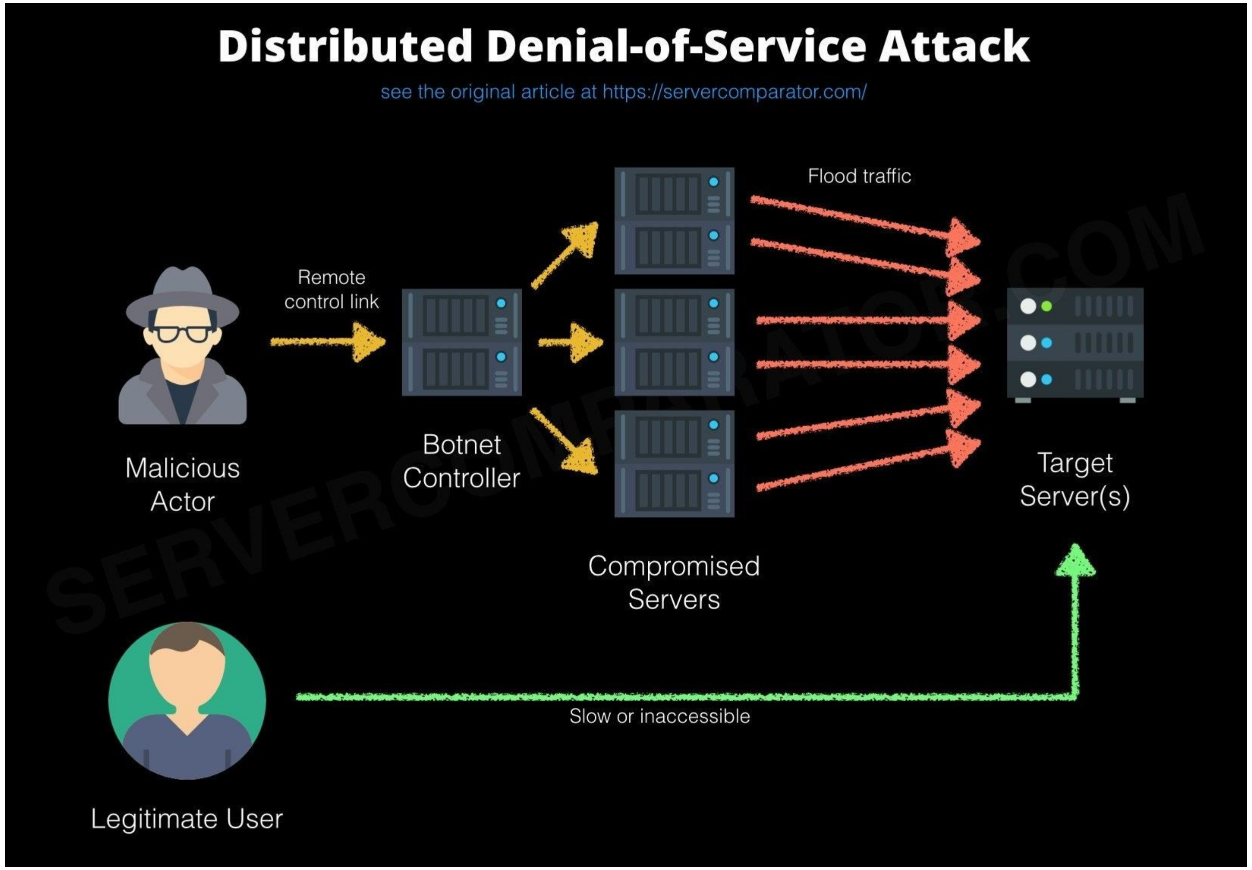
- Manipulating individuals into revealing *confidential data*
- Exremely sucessful:
  - Uber engineers hacked even using MFA (2023)

  - “XZ backdoor” (*April 2024*)
    - The *XZ library* is a cornerstone foundation in the majority of remote computing mechanism (ssh)
    - Implications for “open source” community
    - It took the attacker **more than two years** to finally deploy a malitious code in the project

      https://research.swtch.com/xz-timeline


ALL MODERN DIGITAL INFRASTRUCTURE
tukaani-project / xz
XZ UTILS:
TAKEN OVER BY A BAD ACTOR FOR TWO YEARS AFTER DEVELOPER BURNED OUT
UNICORN RIOT

Types of CyberAttacks
(*advanced “technical” threats*)



- **Denial of Service Attack** (DoS)
- **Distributed-DoS** (DDoS)
- Makes a machine or network resource *unavailable*
- Usually combined with other techniques, such as, “**IP Poisoning**” or “**ARP Spoofing**”)

Information Security Report, 2022-2023
https://security.utoronto.ca/annual-report-2023/

Types of CyberAttacks (*advanced "technical" threats*)

- **Man-in-the-Middle** (MitM)

- Online *eavesdropping*

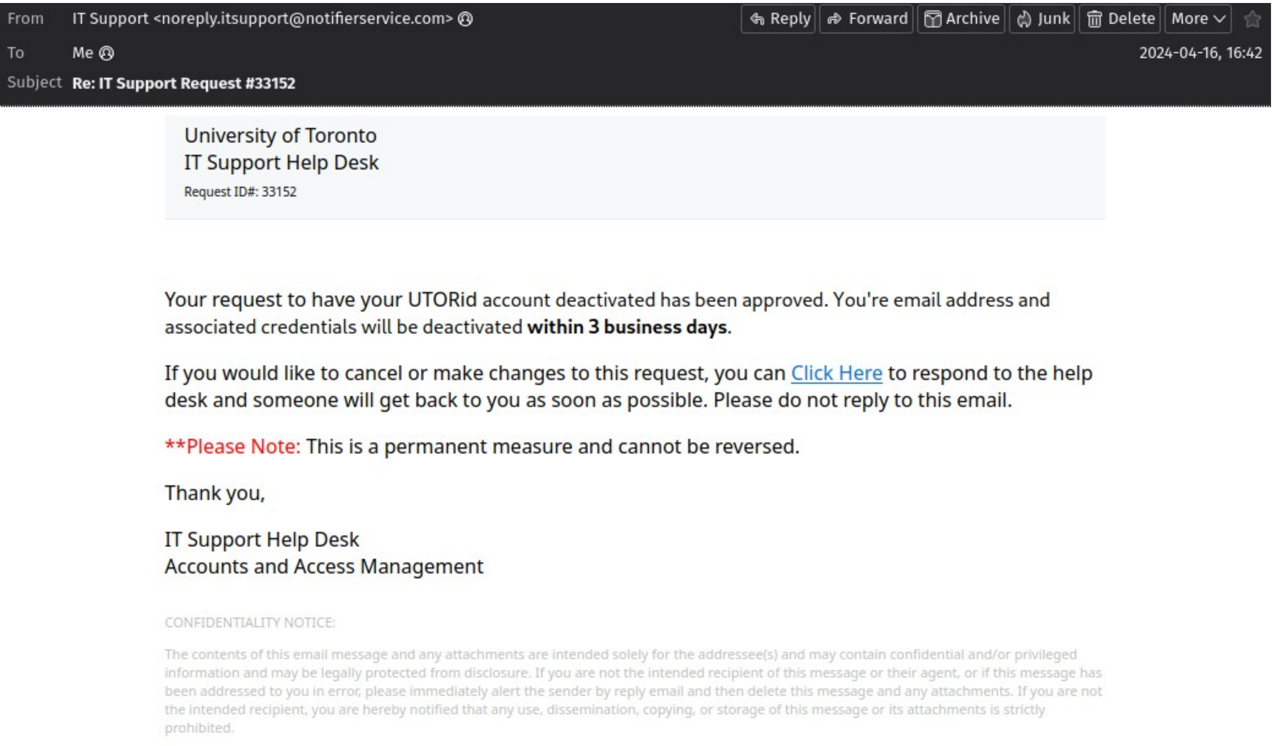
- How to prevent it:
  - **Encryption**
    - **Use https** connections, instead of http

- In particular, be very **careful** when using *public/free wifi*

- How to protect ourselves:
  - Use **VPN**

Quiz #1:

I just received (*true story!*) these two emails: one of them a couple of days ago and the second one yesterday... what do you think abou them?



From IT Support <noreply.itsupport@notifierservice.com>

To Me

2024-04-16, 16:42

Subject **Re: IT Support Request #33152**

University of Toronto
IT Support Help Desk
Request ID#: 33152

Your request to have your UTORid account deactivated has been approved. You're email address and associated credentials will be deactivated **within 3 business days**.

If you would like to cancel or make changes to this request, you can Click Here to respond to the help desk and someone will get back to you as soon as possible. Please do not reply to this email.

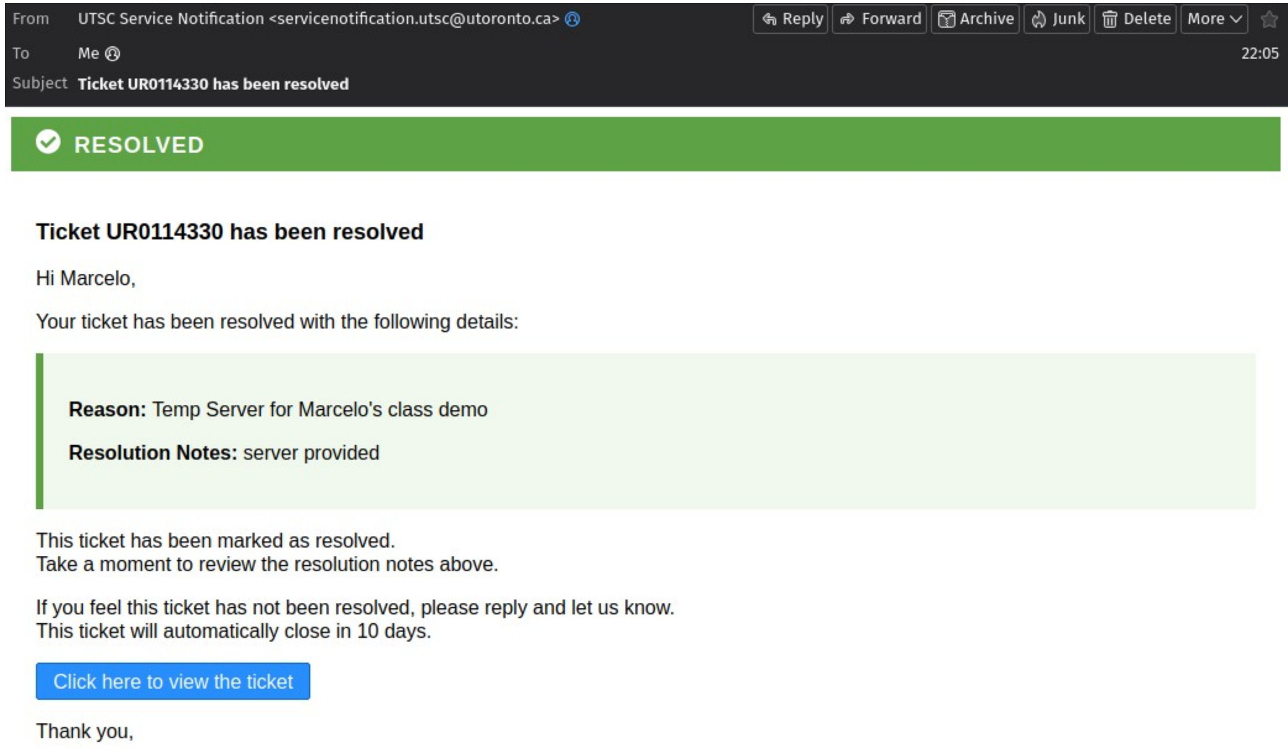
**Please Note: This is a permanent measure and cannot be reversed.

Thank you,

IT Support Help Desk
Accounts and Access Management

CONFIDENTIALITY NOTICE:

The contents of this email message and any attachments are intended solely for the addressee(s) and may contain confidential and/or privileged information and may be legally protected from disclosure. If you are not the intended recipient of this message or their agent, or if this message has been addressed to you in error, please immediately alert the sender by reply email and then delete this message and any attachments. If you are not the intended recipient, you are hereby notified that any use, dissemination, copying, or storage of this message or its attachments is strictly prohibited.



From UTSC Service Notification <servicenotification.utsc@utoronto.ca>

To Me

22:05

Subject **Ticket UR0114330 has been resolved**

✓ RESOLVED

Ticket UR0114330 has been resolved

Hi Marcelo,

Your ticket has been resolved with the following details:

Reason: Temp Server for Marcelo's class demo

Resolution Notes: server provided

This ticket has been marked as resolved.
Take a moment to review the resolution notes above.

If you feel this ticket has not been resolved, please reply and let us know.
This ticket will automatically close in 10 days.

Click here to view the ticket

Thank you,

Things to notice:

- minor typos, sense of urgency, ...
- always consider if the information/request is reasonable ...
- check some technical insights, e.g. “headers”, hop over (**do NOT click!**) on hyperlinks ...

Resources I

- **Security Awareness and Training Program (SATP)**

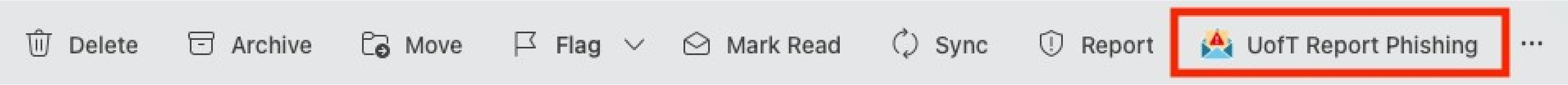
- Enrollment is by request, for faculty and staff

  https://www.utsc.utoronto.ca/iits/security-awareness-training-program
  https://security.utoronto.ca/cyberstrategy/strategic-initiatives/satp/

U of T Report Phishing button

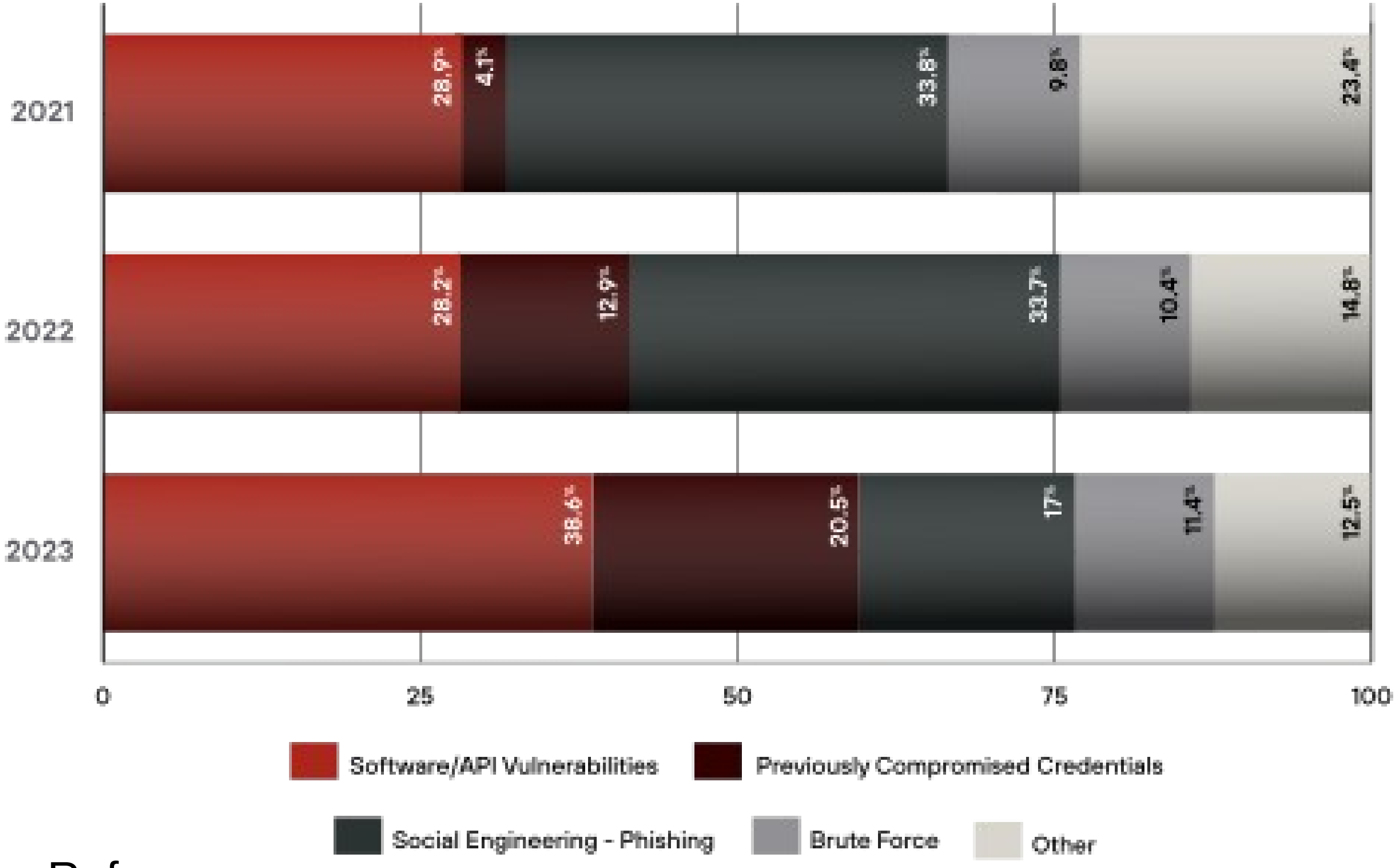
https://securitymatters.utoronto.ca/uoft-report-phishing-button/

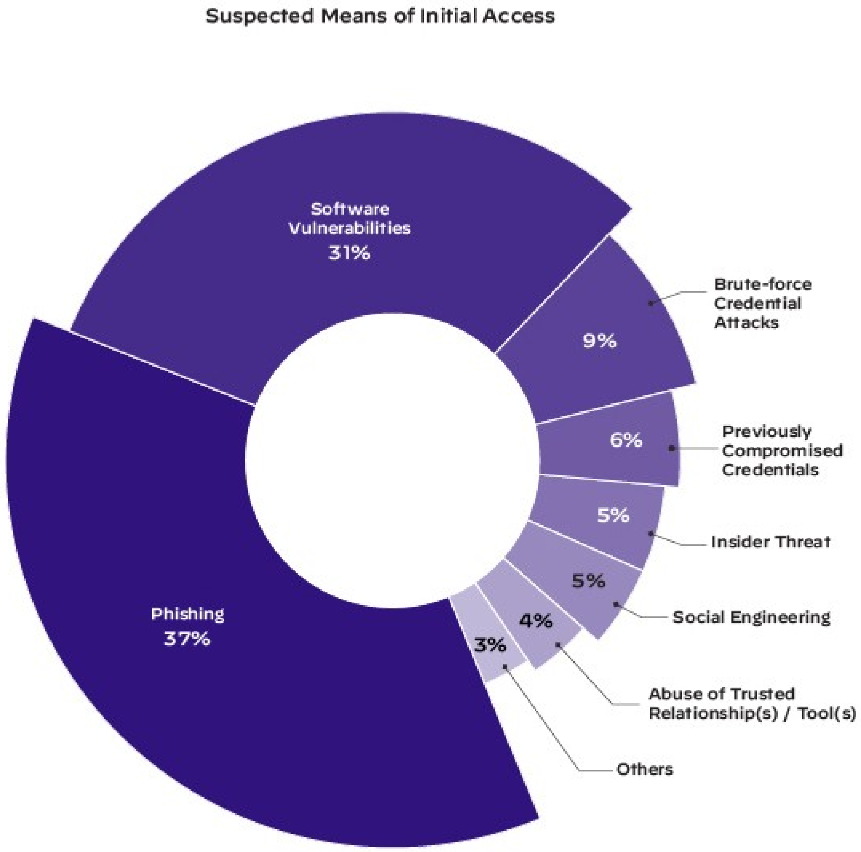
report.phishing@utoronto.ca



Protecting Our Information (*digital assets*)

Protecting Our Systems





TOP 4 INITIAL ACCESS VECTORS FROM UNIT 42 INCIDENT RESPONSE CASES IN 2023

Ref.

https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report
https://unit42.paloaltonetworks.com/incident-response-report/

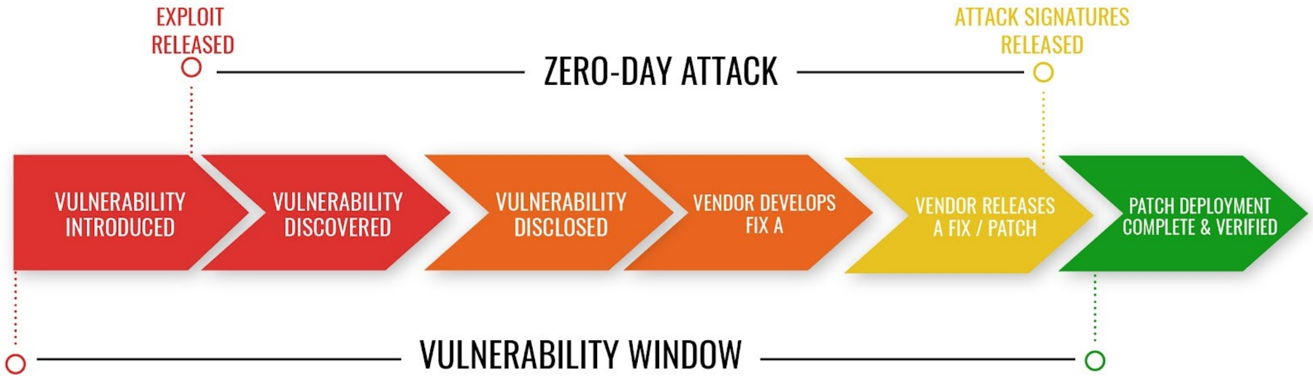
Protecting Our Systems I – **Software Updates**

Self-reflecting question…

How often do you ***update*** your computing devices?

Why is this important/relevant?

=> **Zero-day exploits**



But… I am using multi-factor authentication!

But… I am using a VPN!

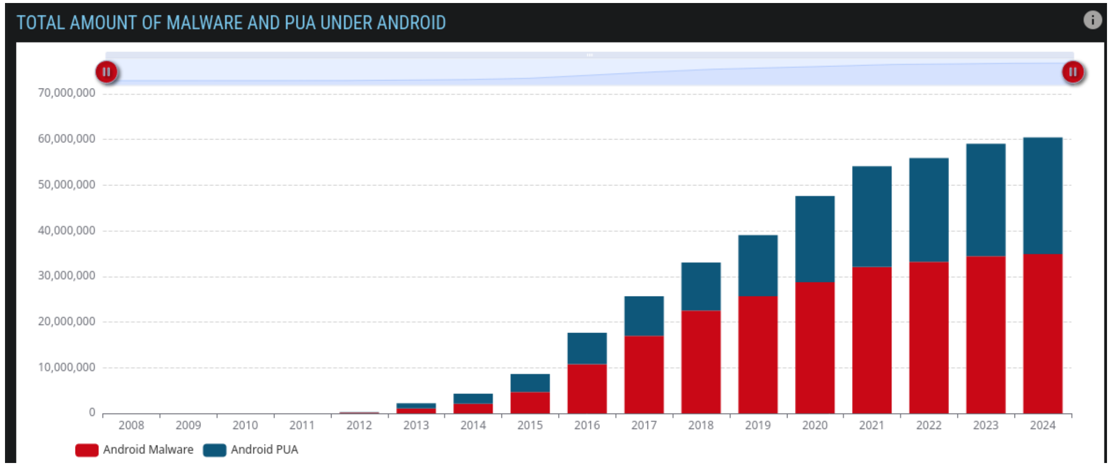
But… I am only browsing on websites I know!

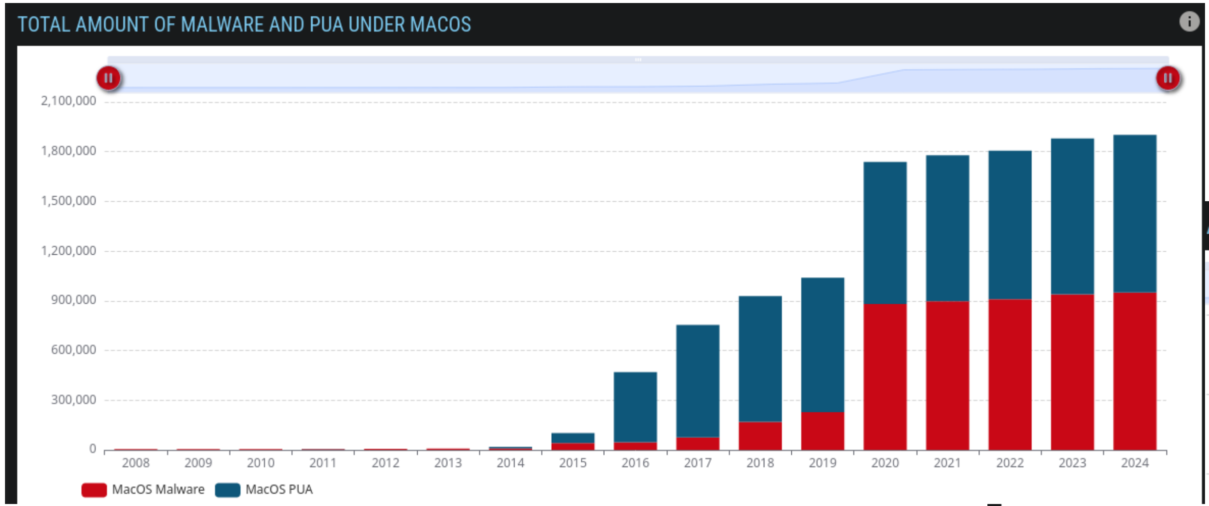
YES – WE STILL NEED TO UPDATE OUR SYSTEMS!

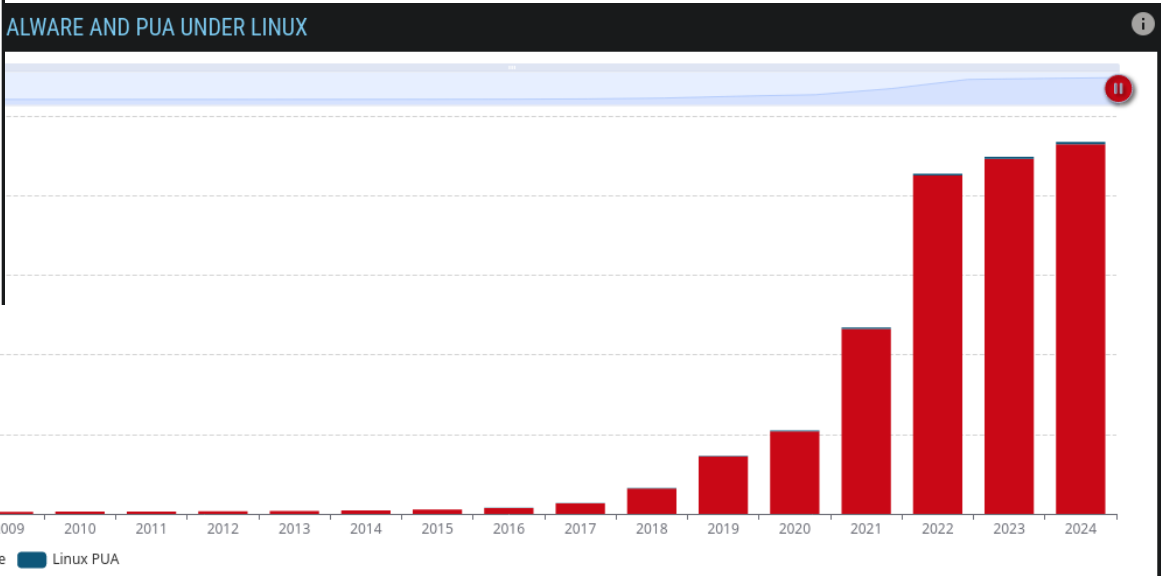
Protecting Our Systems II – **Anti-Malware/Viruses**

Another self-reflecting question…

Do you use an antivirus?





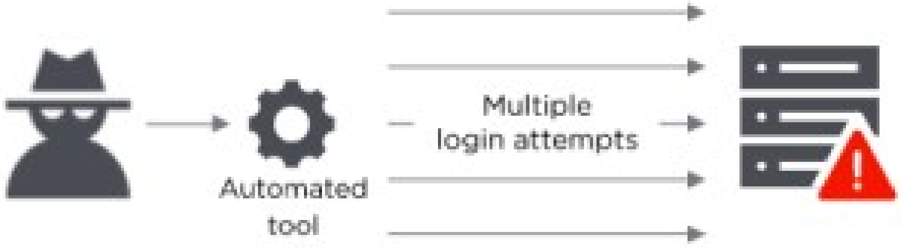


https://cybermap.kaspersky.com/

Src: https://portal.av-atlas.org/

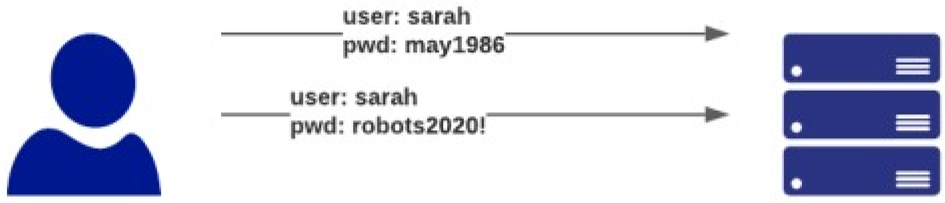
Protecting Our Systems III – **Password Attacks**

- Brute force attacks
- Dictionary attacks
- Keyloggers
- Password "guessing"
- Password spraying
- Phishing



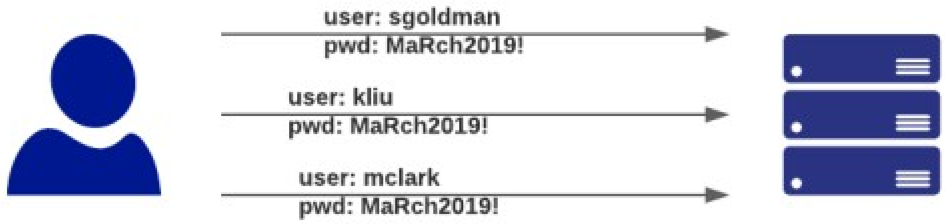
Multiple login attempts

Automated tool



user: sarah
pwd: may1986

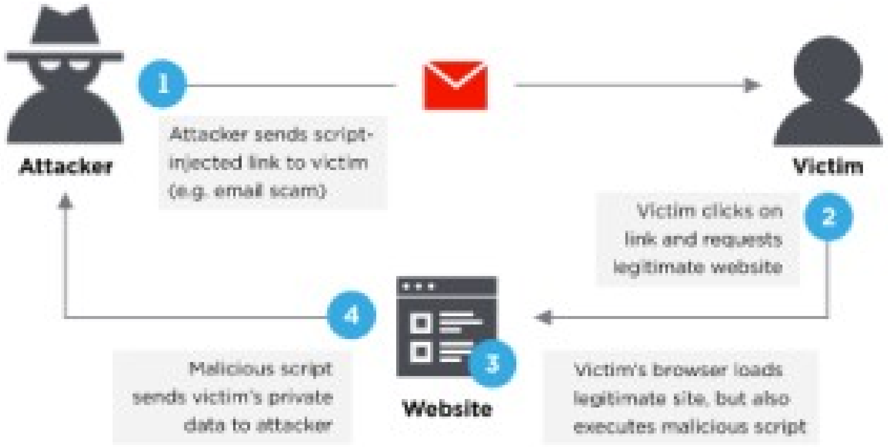
user: sarah
pwd: robots2020!



user: sgoldman
pwd: MaRch2019!

user: kliu
pwd: MaRch2019!

user: mclark
pwd: MaRch2019!



Attacker

Victim

Website

1 Attacker sends script-injected link to victim (e.g. email scam)

2 Victim clicks on link and requests legitimate website

3 Victim's browser loads legitimate site, but also executes malicious script

4 Malicious script sends victim's private data to attacker

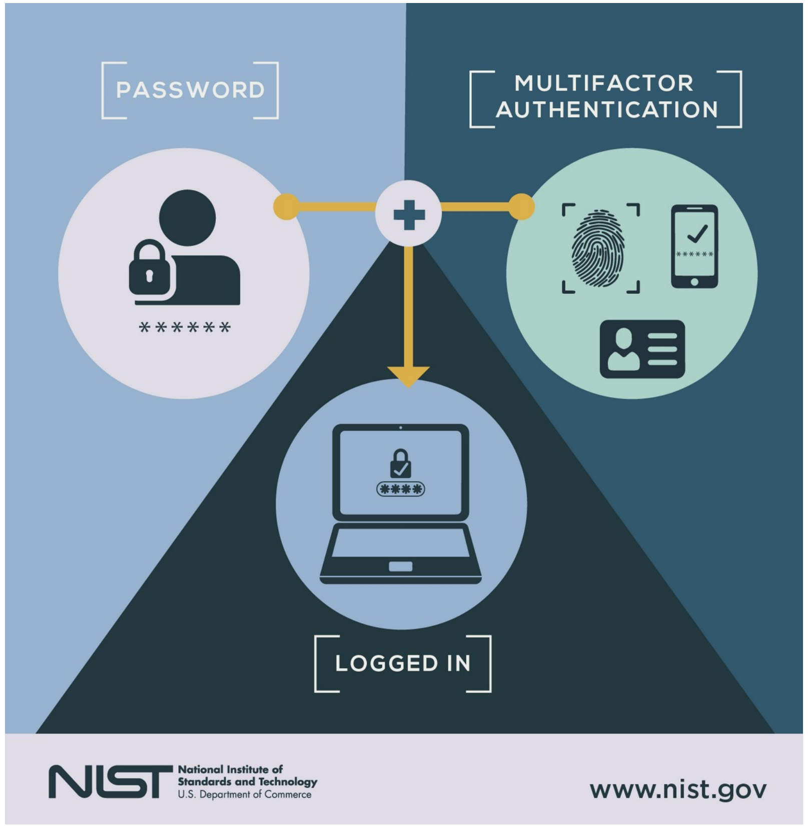
Best Practices – **Passwords Strategies**

- Do **not** use the same password everywhere
- Do **not** use simple passwords (example: Summer2018)
- Do **not** store passwords in clear text
- Do **not** share your password
- Do **not** transmit password via email or text

- Use complex passwords (mix of letters, numbers, symbols).
- Use a different password for each account
- Use a password vault, such as
- LastPass, Bitwarden, Keypass
- Long passphrase (15 characters or more)
- Use **MFA** (multi-factor authentication) when possible
- Transmit securely: **encrypt** sensitive files and communications.

Best Practices – **Use Multi-Factor Authentication**

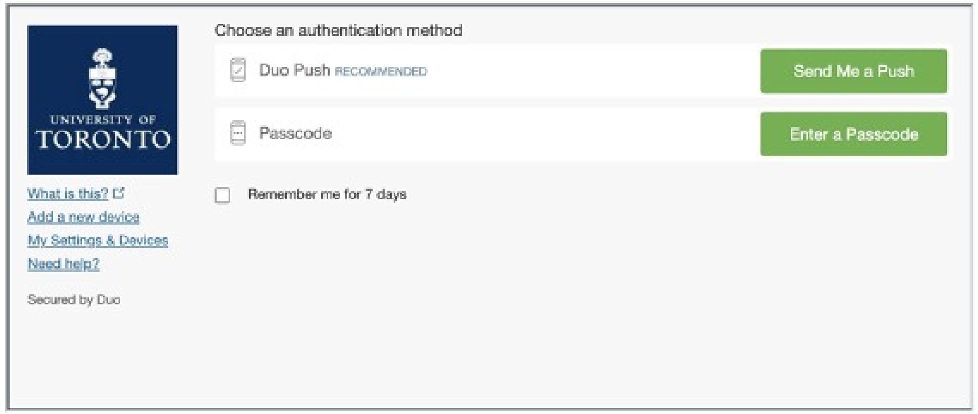
- **Multi-Factor Authentication (MFA):** provide several pieces of evidence from different factors to prove your identity
- Factors:
  - Something you know
  - Something you have
  - Something you are
- Protection against phishing, social engineering and password brute-force attacks and stolen credentials


PASSWORD
******
MULTIFACTOR AUTHENTICATION
******
****
LOGGED IN
NIST National Institute of Standards and Technology U.S. Department of Commerce
www.nist.gov

https://www.nist.gov/itl/applied-cybersecurity/back-basics-multi-factor-authentication-mfa

Best Practices – **MFA Variants**

- There are multiple ways in which MFA (aka 2FA) can be implemented/used
- Examples: DUO (uoft), google-authenticator, etc.
- It is possible to use a *hardware-key* in combination with your MFA.
  E.g. Yubikeys



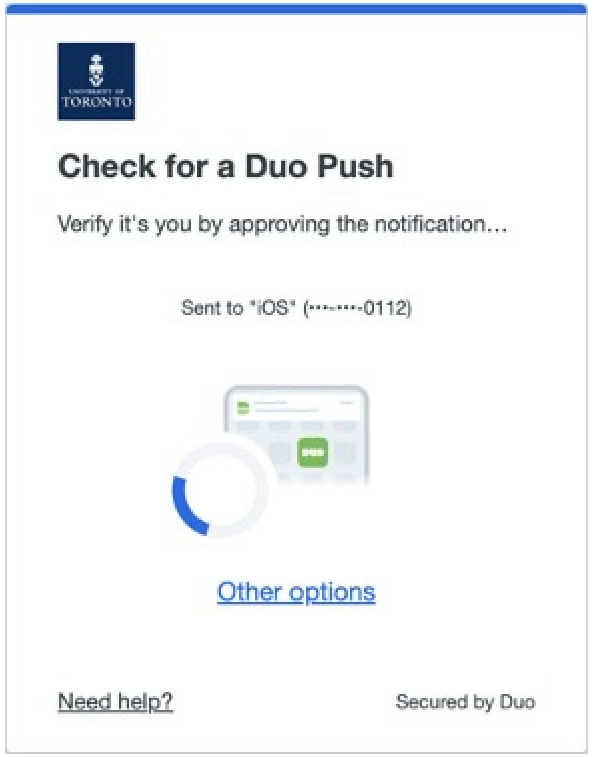
Choose an authentication method

Duo Push RECOMMENDED — Send Me a Push

Passcode — Enter a Passcode

□ Remember me for 7 days

https://security.utoronto.ca/services/utormfa/



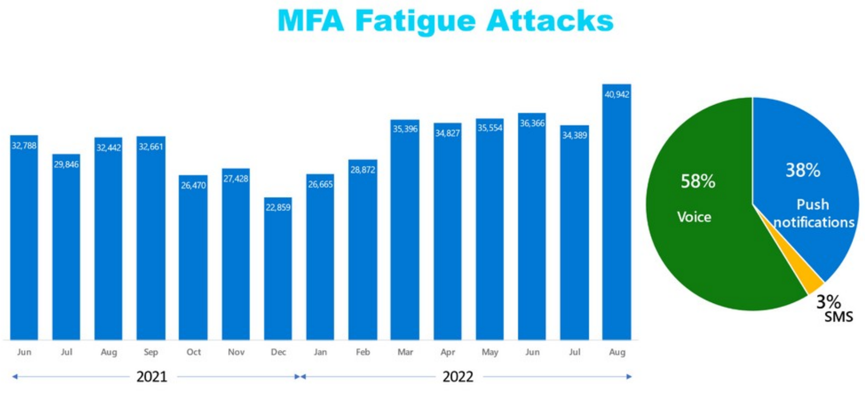
Check for a Duo Push

Verify it's you by approving the notification...

Sent to "iOS" (•••-•••-0112)

https://www.yubico.com/

Best Practices – **MFA, final comments**



Source: Azure AD Identity Protection sessions at high risk with multiple failed MFA attempts

- Stealing *cookies* is one method to circumvent MFA.
- Some MFA factors are more robust than others.
- MFA-fatigue …
  https://techcommunity.microsoft.com/t5/microsoft-entra-blog/defend-your-users-from-mfa-fatigue-attacks/ba-p/2365677

While MFA is one efficient and additional way to protect your research, adopting the principle of *in-depth defense* is essential (i.e. regular patching, have an anti-virus, being careful of phishing etc…):

if one control fails, another control protects your systems/data – redundancy in-place!

Best Practices – **Safe Internet Browsing**

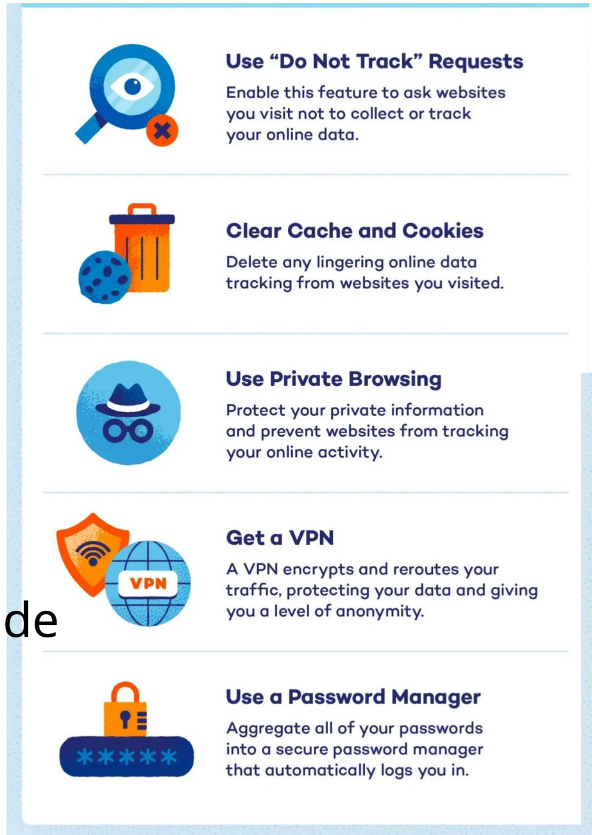
> Consider the Internet an **unsafe** place by default!

- **Public-WIFI: avoid it as much as possible**
- If you absolutely need to access a public WIFI:
  - Ensure that the WIFI name is known
  - Consider using a VPN (Virtual Private Network)
  - Check for **https** websites and *certificates*
  - Personal information: be mindful of what you provide

    Name, address, phone number, date of birth,…
- Be careful with browser extensions/plugins, and browsers in general (*Brave*)
- Not sure about the legitimacy of a website?

  https://www.virustotal.com
- Use Cira Canadian Shield at home

  https://www.cira.ca/en/canadian-shield/



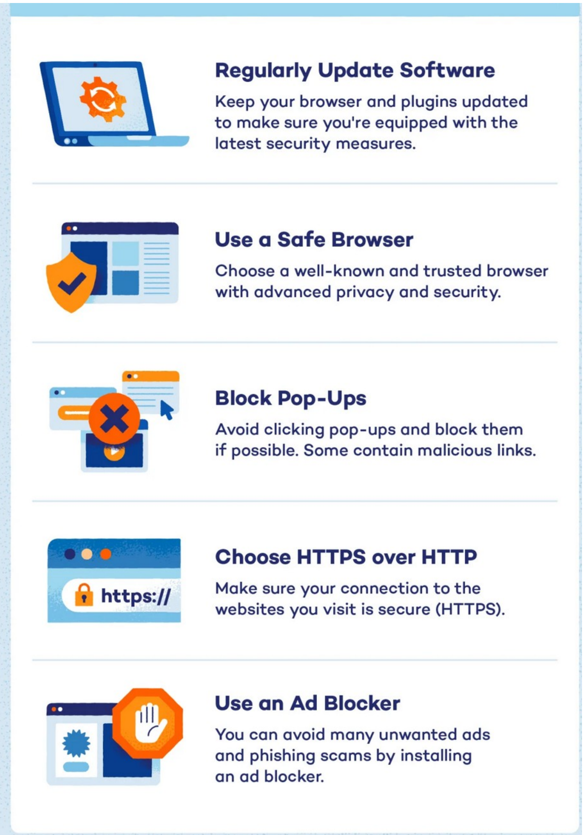
Use "Do Not Track" Requests
Enable this feature to ask websites you visit not to collect or track your online data.

Clear Cache and Cookies
Delete any lingering online data tracking from websites you visited.

Use Private Browsing
Protect your private information and prevent websites from tracking your online activity.

Get a VPN
A VPN encrypts and reroutes your traffic, protecting your data and giving you a level of anonymity.

Use a Password Manager
Aggregate all of your passwords into a secure password manager that automatically logs you in.



Regularly Update Software
Keep your browser and plugins updated to make sure you're equipped with the latest security measures.

Use a Safe Browser
Choose a well-known and trusted browser with advanced privacy and security.

Block Pop-Ups
Avoid clicking pop-ups and block them if possible. Some contain malicious links.

Choose HTTPS over HTTP
Make sure your connection to the websites you visit is secure (HTTPS).

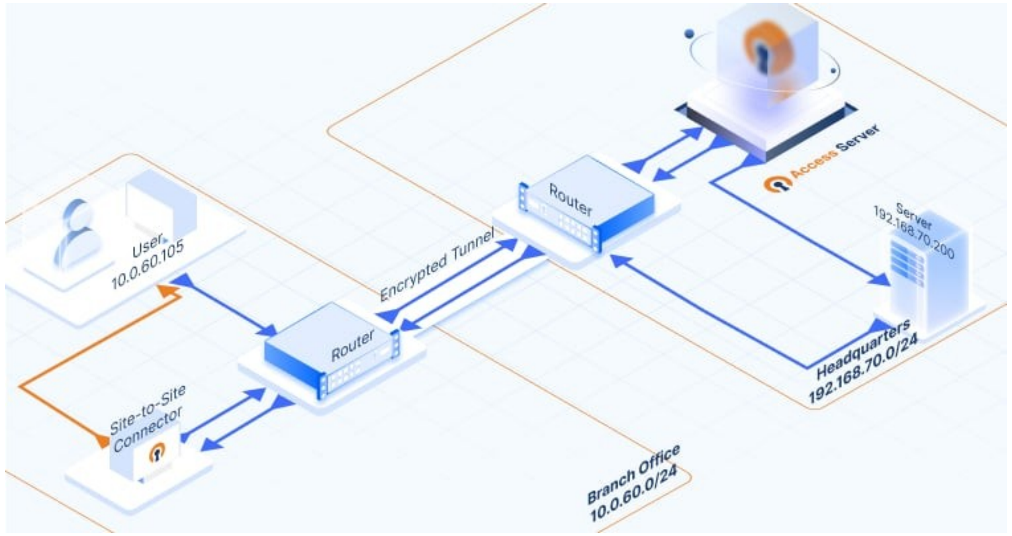
Use an Ad Blocker
You can avoid many unwanted ads and phishing scams by installing an ad blocker.

Best Practices – **VPN: Virtual Private Network**

- *Encrypted* connection between the user’s device and the Internet
- Provides online *privacy* and *anonymity* by masking the user’s IP address
- Minimizes two main risks:
    - Privacy risk, as a VPN provides anonymity
    - Someone eavesdropping your connection (MitM)
- Available via your host institution, or often included as part of anti-malware vendor service

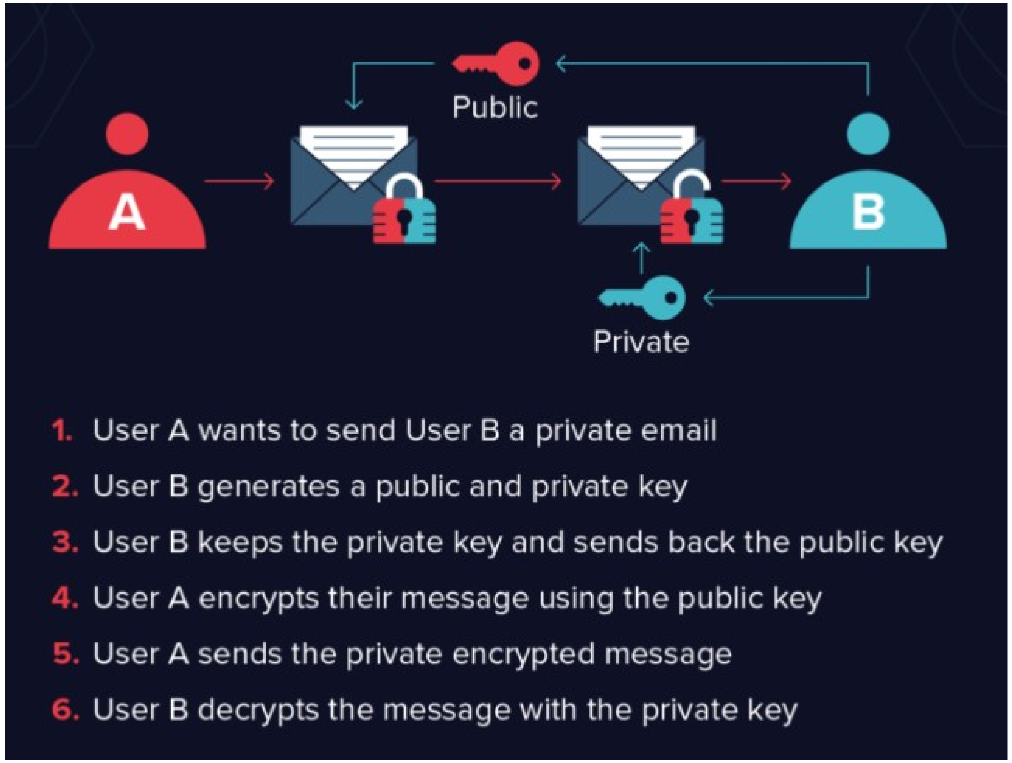
    https://isea.utoronto.ca/services/vpn/utorvpn/

- Regulations in some countries



Best Practices – **Backups, Encryption, …**

- **Backup** your important data on a *regular basis*
- Keep your backups in a safe, *different* location
- Cloud *vs* on-premise
- Test your backups!
- Different types of backup:
  full, differential, incremental
- Email is **NOT** a backup



1. User A wants to send User B a private email
2. User B generates a public and private key
3. User B keeps the private key and sends back the public key
4. User A encrypts their message using the public key
5. User A sends the private encrypted message
6. User B decrypts the message with the private key

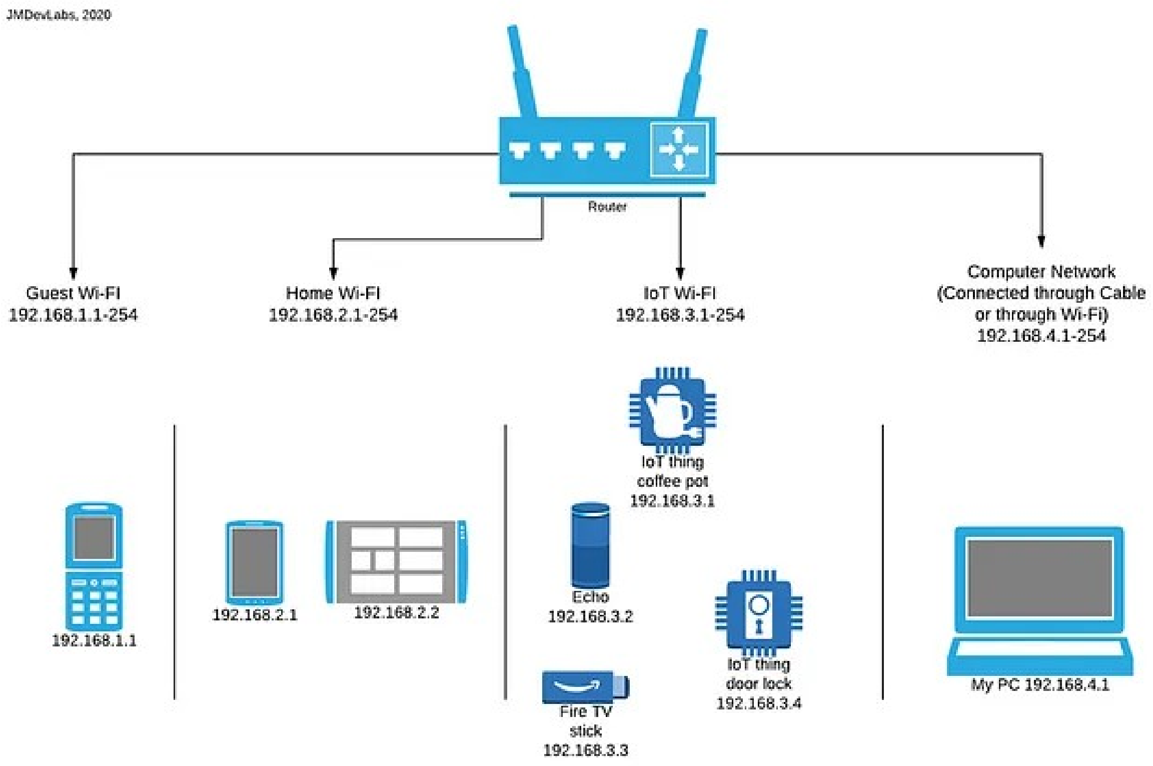
Best Practices – **Some final thoughts…**

> Home network, IoT (smart devices, peripherials):

  - *Network segmentation*: public sector, private sector
  - Keep things updated!

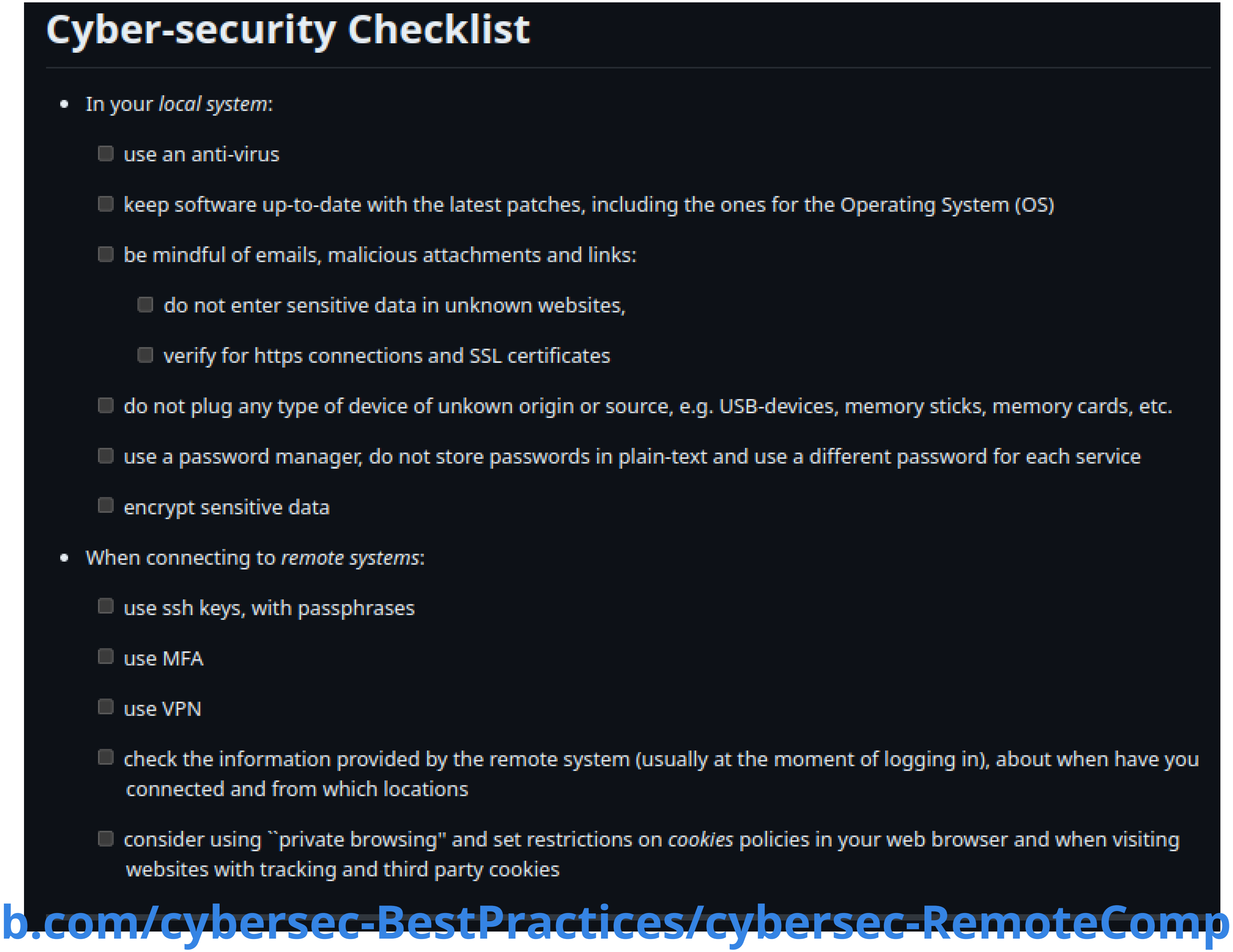
> email:

- Unsecure, unencrypted!
- Encryption is available, e.g. via PGP (Pretty Good Privacy)



JMDevLabs, 2020
Router
Guest Wi-FI 192.168.1.1-254
Home Wi-FI 192.168.2.1-254
IoT Wi-FI 192.168.3.1-254
Computer Network (Connected through Cable or through Wi-Fi) 192.168.4.1-254
IoT thing coffee pot 192.168.3.1
192.168.1.1
192.168.2.1
192.168.2.2
Echo 192.168.3.2
IoT thing door lock 192.168.3.4
Fire TV stick 192.168.3.3
My PC 192.168.4.1

Best Practices – **CyberSecurity Checklist**



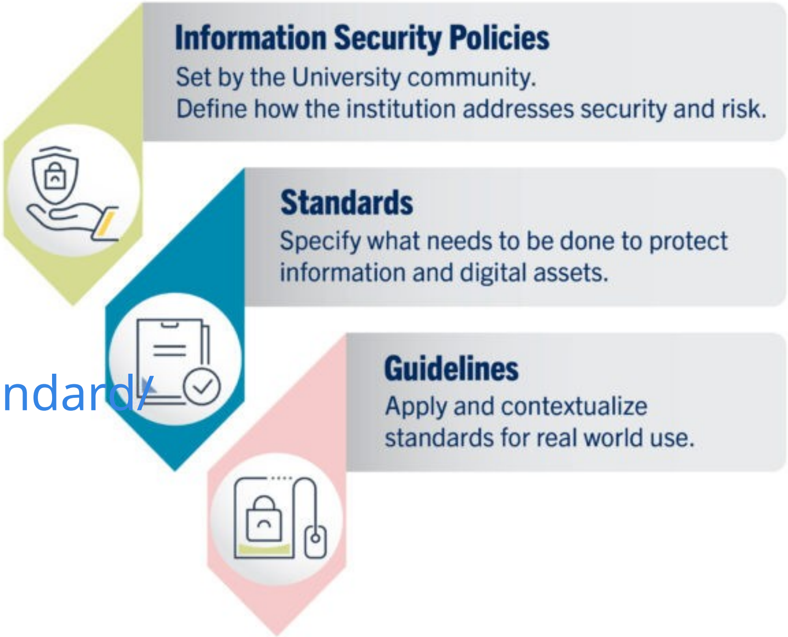
Cyber-security Checklist

- In your *local system*:
  - □ use an anti-virus
  - □ keep software up-to-date with the latest patches, including the ones for the Operating System (OS)
  - □ be mindful of emails, malicious attachments and links:
    - □ do not enter sensitive data in unknown websites,
    - □ verify for https connections and SSL certificates
  - □ do not plug any type of device of unkown origin or source, e.g. USB-devices, memory sticks, memory cards, etc.
  - □ use a password manager, do not store passwords in plain-text and use a different password for each service
  - □ encrypt sensitive data
- When connecting to *remote systems*:
  - □ use ssh keys, with passphrases
  - □ use MFA
  - □ use VPN
  - □ check the information provided by the remote system (usually at the moment of logging in), about when have you connected and from which locations
  - □ consider using ``private browsing'' and set restrictions on *cookies* policies in your web browser and when visiting websites with tracking and third party cookies

https://github.com/cybersec-BestPractices/cybersec-RemoteComputing/

Legal Considerations

Information Security – Policies, Standards and Guidelines



Information Security Policies
Set by the University community.
Define how the institution addresses security and risk.

Standards
Specify what needs to be done to protect information and digital assets.

Guidelines
Apply and contextualize standards for real world use.

- Data Classification Standard
  https://security.utoronto.ca/framework/standards/data-classification-standard/
  - 4 levels: L1-to-L4
    eg. Level-4: SIN, PHIPA
  - Handling of data of level-4, e.g. SIN --
    https://security.utoronto.ca/framework/standards/data-classification-standard/interpretive-guidance-sins/

- https://security.utoronto.ca/framework/

Conclusions

Concluding Remarks

- *Cybersecurity* is the **practice** of protecting computer systems, networks, and data from theft, damage, or unauthorized access.
- In reality, represents our efforts and attempts to **mitigate** *attacks and threats.*
- In our interconnected world, cybersecurity is crucial to safeguard personal information, research assets, and critical infrastructure.
- Cybersecurity as it is usually refer to is a *moving target:* i.e. it implies dynamic and fluid adaptation to ever-changing circumstances.
- However, one element that is and will remain to be critical is the *human factor*!

We have left out many interesting and important topics:

- encryption, AI, remote computing, training and education (awareness),
  quantum computing, etc.

THANK YOU!

Resources & References

REFERENCES

- DDoS -- https://www.cyber.gc.ca/en/guidance/distributed-denial-service-attacks-prevention-and-preparation-itsap80110

- "Cybersecurity Training for Users of Remote Computing", **MP**, R.vanZon; JOCSE (2023) https://doi.org/10.22369/issn.2153-4136/14/2/3

RESOURCES

- UofT *Security Matters*
  https://securitymatters.utoronto.ca/

- *Security Awareness and Training Program (SATP)*
  https://www.utsc.utoronto.ca/iits/security-awareness-training-program
  https://security.utoronto.ca/cyberstrategy/strategic-initiatives/satp/

- Check if your credentials have been compromised
  https://haveibeenpwned.com/

- CyberSecurity Best Practices Repository
  https://github.com/cybersec-BestPractices

- https://science.gc.ca/site/science/en/safeguarding-your-research