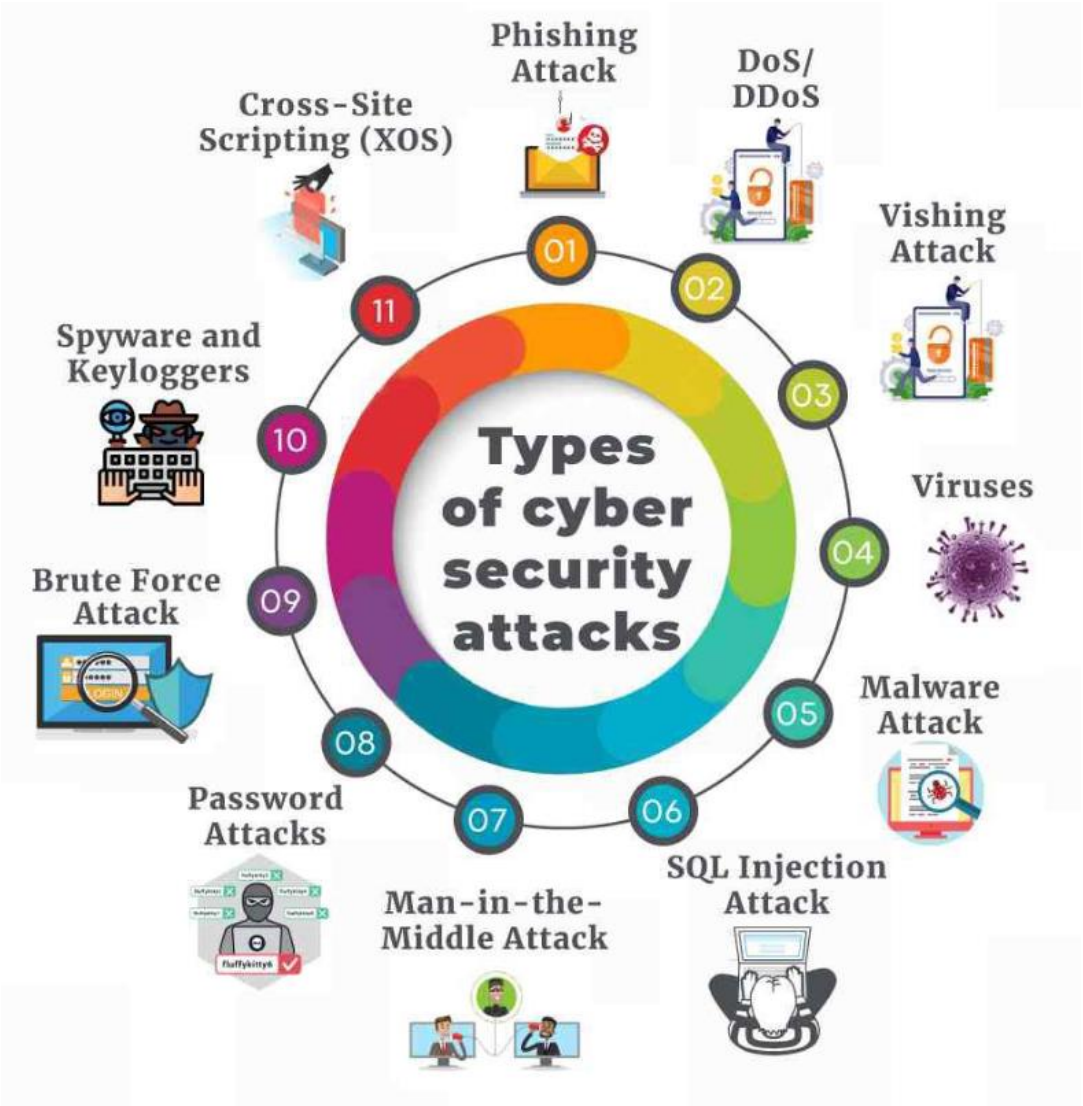
Cyber Attack

- A **cyber attack** is a set of actions that is carried out by **treat actors** in order to gain ***unauthorized access***, ***steal data***, or ***cause damage*** to computers, computer networks, or other computing resources.
- Treat actors can be called cybercriminals, hackers, or bad actors.
- Cyber criminals try to find **vulnerabilities**, that is ***weakness, problems***, or ***limitations*** in computer systems to exploit them for achieving further goals.
- Cybercriminals can have various motivations for attacks: financial gain, personal, hacktivism in the name of social or political causes, and part of cyberwarfare operations carried out by nation states against their opponents.

Ref: https://www.istockphoto.com/illustrations/cartoon-graphic-of-a-thief-with-a-laptop-cyber-crime

Classification of Cyber Attacks

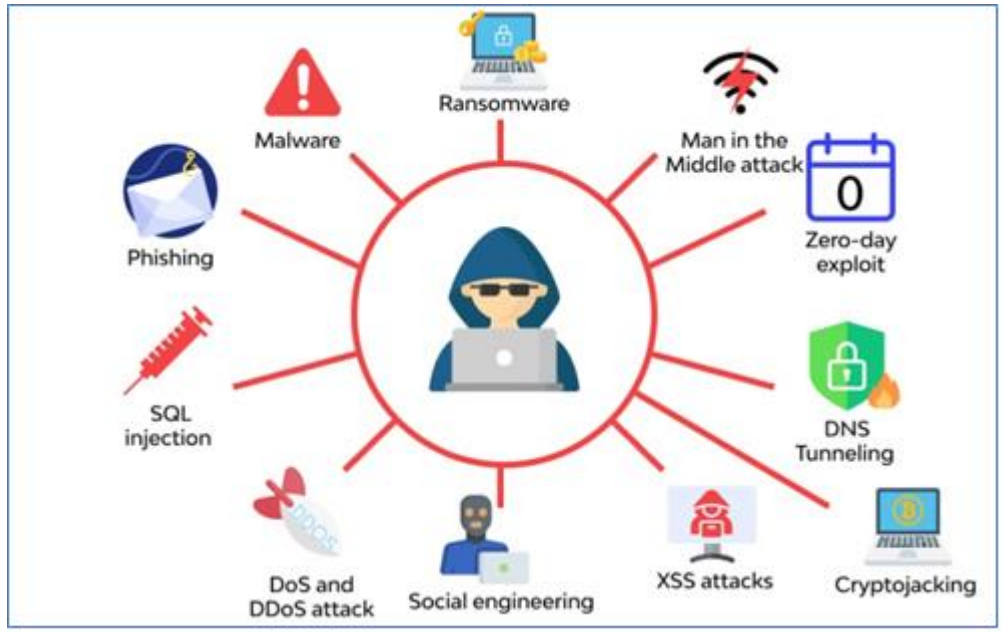


Ref: https://malaykaushik2000.medium.com/cyber-crime-and-information-about-confusion-matrix-and-its-two-types-of-errors-b74e34d444c2

Malware

Malware

- Malware (short for Malicious Software) are used for various goals, including stealing information, creating persistent access to a network, defacing or altering web content, and damaging a computing system permanently.
- One of the most common attack technique.
- Different types of malware:
  - Viruses
  - Worms
  - Trojans
  - Ransomware
  - Spyware
  - Keyloggers

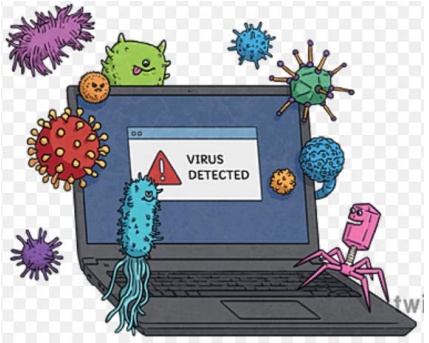


Ref: https://www.wallarm.com/what/what-is-a-cyber-attack

Malware

Viruses

- A computer virus is a program code that is attached to another program and file and is activated when the program is executed, or the file is opened.
- Viruses can self-replicate without the knowledge of the victim and can be used to carry out various attacks, such as stealing data, slowing down device, providing unauthorized access to devices, etc.



https://www.twinkl.com.bh/illustration/Computer-Virus-png

Worms

- A special type of virus that can travel throughout a network from one infected device to another and replicate itself.
- Usually, worms do not harm a system directly, rather provides hackers remote access to the entire system or network.

https://www.emsisoft.com/en/blog/28154/computer-worms/

Malware

Trojans

- Trojan or **Trojan Horse** is a type of malware that disguises itself as a legitimate/useful software.
- One installed, the malware can carry out any legitimate actions, such as changing data, exporting files, destroying data, and so on.
- Example: downloading and installing a trojan as a free anti-virus software.

https://codesealer.com/how-financial-trojan-can-bad-impact-your-business/

Spyware

- A malware that runs in the background by hiding itself and gathers user's activities and sends activity or sensitive data back to the hacker.
- Sensitive data can include login credentials and banking details.

https://izoologic.com/2018/11/08/start-spyware-company-germany-accidentally-exposed-data-online/

Malware

https://blog.ariacybersecurity.com/blog/just-what-is-a-ransomware-attack-and-can-you-prevent-one

Ransomware

- Malware that encrypts files on the victim's device and demands to pay a ransom (usually in cryptocurrency) in return of the files in original state.
- It is reported that there was an 80% increase year-over-year in ransomware attacks worldwide in 2022.

https://nordvpn.com/blog/keylogger-protection/

Keyloggers/Keystroke Loggers

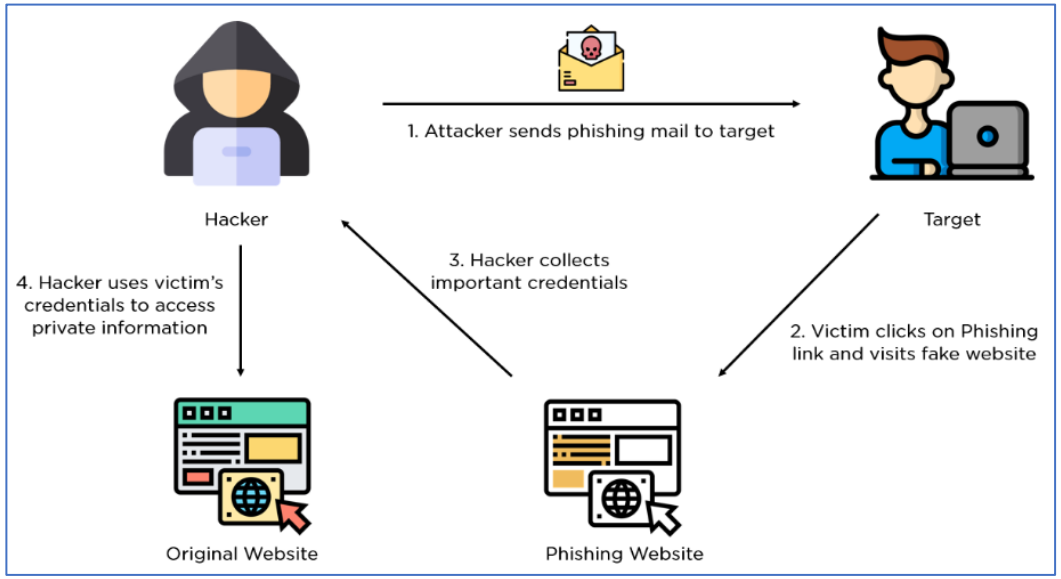
- Everything a user types on a system is recorded by the keylogger.
- Keyloggers can have legitimate use, e.g., management can track employees' activities within the office workstations.
- However, can also be used for malicious purpose and can send each key stroke information to attackers that can be used to carry out attacks such as blackmailing or identity theft.

Prevention of Malware Attacks

- Ensure that you have the latest and most effective anti-malware/spam protection software installed.
- Ensure that your staff is trained to identify malicious emails and websites.
- Have a strong password policy and use multi-factor authentication where possible.
- Keep all software patched and up-to-date.
- Only use administrator accounts when absolutely necessary.
- Control access to systems and data, and strictly adhere to the least-privilege model.
- Monitor your network for malicious activity, including suspicious file encryption, inbound/outbound network traffic, performance issues, and so on.

Phishing Attacks

- A type of cyber attack where cybercriminals send messages pretending to be a trusted person and entity.
- Phishing attacks are carried out via fraudulent emails, text/SMS (called **Smishing**), or phone call (called **Vishing**).
- Messages are prepared in such a way that they look like they're from someone official or a person or business that the victim trusts, e.g., bank, tax office, police, national intelligence agency, companies like Microsoft, Telco, ISP, Netflix, etc.
- Phishing/Smishing message may ask the victim to click/tap on an external link or open an attachment which may download malware or take the victim to phishing site that can stead victim's sensitive data.



https://www.simplilearn.com/tutorials/cryptography-tutorial/what-is-phishing-attack

The Biggest Phishing Breaches of 2022 and How to Avoid them for 2023
https://securityboulevard.com/2022/11/the-biggest-phishing-breaches-of-2022-and-how-to-avoid-them-for-2023/#:~:text=Twilio%20(August%202022),resembling%20Twilio's%20real%20authentication%20site.

Phishing Attacks

- Generally phishing attacks target a wide range of victims that makes it easy to identify.
- However, recently targeted phishing attacks are carried out that are harder to investigate.

Spear Phishing Attacks

- Targets a specific individual and carried out via email.
- Cybercriminals collect personal information from social media, online footprints, or Dark Web, and prepare personalized message to persuade the target click/tap on the phishing link.

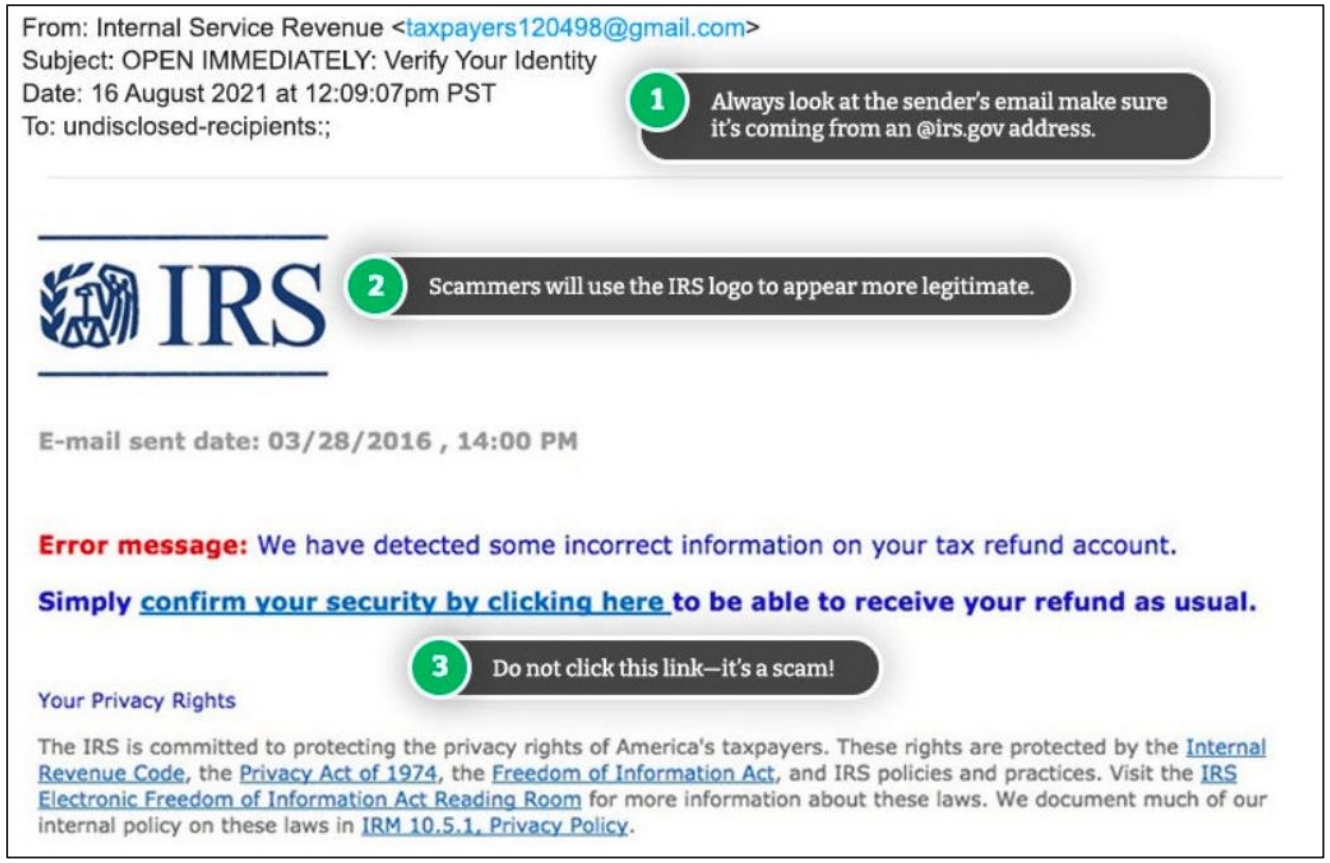
Whaling

- A phishing attack that targets high-profile personalities, such as CEOs, MDs, executive officers.
- The objective of such attacks is to collect their credentials and get access to the company network.

Angler Phishing Attack

- A new type of phishing scam where attacker baits target users on social media pretending to be a well-known companies customer service consultant/account.
- Example: Scammers create accounts like "@AmazonHelp$" and then auto-respond to relevant messages by providing a link for the target to talk to a customer service consultant.

Phishing Attacks



An example of a phishing email claiming to be from the IRS (Tax office in US)

Ref: https://www.aura.com/learn/types-of-cyber-attacks

Rule of Thumb

- Always question unsolicited messages, in particular coming from Large Organizations, Govt. Agencies, Telcos, etc.
- Always verify the message first by contacting the organization by obtaining the correct contact information instead of further engaging with the message.

Prevention of Phishing Attacks

1) Know what a phishing scam looks like

- New phishing attack methods are being developed all the time, but they share commonalities.
- Know latest phishing tactics:

  https://securityboulevard.com/2022/11/the-biggest-phishing-breaches-of-2022-and-how-to-avoid-them-for-2023/

  https://portswigger.net/daily-swig/phishing

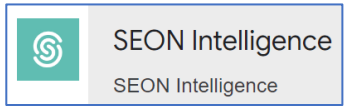
2) Don't click unsolicited link

- It is generally advised to not click on the link, the bare minimum you should do is hovering over the link to see if the destination is the correct one.
- Better to go straight to the site through search engine, rather than clicking on the link.

3) Get anti-phishing add-ons (free!)

- Most browsers nowadays will enable you to download add-ons that spot the signs of a malicious website or alert you about known phishing sites.
- Top 9 Chrome Extensions for Fraud Detection & Prevention 2023

  https://seon.io/resources/comparisons/best-fraud-detection-chrome-extensions/



Prevention of Phishing Attacks

4) Don't give your information to an unsecured site

- If the URL of the website doesn't start with "https", or a closed padlock icon next to the URL is not visible, do not enter any sensitive information or download files from that site.

Chrome		Firefox	Edge
Not secure | bom.gov.au	knowbe4.com/	https://login.my.gov.au/	https://nbr.gov.bd

5) Rotate passwords regularly

- Changing passwords of online accounts regularly protects accounts from password attacks.

6) Don't ignore those updates

- Security patches and updates are released for a reason, most commonly to keep up to date with modern cyber-attack methods by patching holes in security.

7) Install firewalls

- Both desktop firewalls and network firewalls, when used together, can bolster the security and reduce the chances of a hacker infiltrating the network and individual computers.

Prevention of Phishing Attacks

8) Don't be tempted by the pop-ups

- Pop-ups are often linked to malware as part of attempted phishing attacks.
- Free ad-blocker software can automatically block most of the malicious pop-ups.
- Occasionally pop-ups will try and deceive you with where the "Close" button is, so always try and look for an "x" in one of the corners.

StayFree - Website Blocker & Web Analytics
stayfreeapps.com Featured

Guardio

uBlock Origin
Offered by: Raymond Hill (gorhill)

AdBlock

Adblock Plus

9) Don't give out important information unless you must

- As a general rule of thumb, unless you 100% trust the site you are on, you should not willingly give out your card information.

10) Have a Data Security Platform to spot signs of an attack

- In case of a successful phishing attack, it's important it is detected and reacted in a timely manner.
- Having a data security platform in place helps take some of the pressure off the IT/Security team by automatically alerting on anomalous user behavior and unwanted changes to files.

References

Cyber Attacks

- https://www.imperva.com/learn/application-security/cyber-attack/
- https://www.aura.com/learn/types-of-cyber-attacks
- https://www.lepide.com/blog/the-15-most-common-types-of-cyber-attacks/
- https://www.lepide.com/blog/10-ways-to-prevent-phishing-attacks/