Common Cyber Threats and Attacks

GEORGIA TECHNOLOGY AUTHORITY

NCSAM 2023

Watch Your Back!

A cyber threat refers to any potential harm that can occur using digital technology or cyberspace. These threats encompass a wide range of malicious activities and actions carried out by cybercriminals, hackers, or threat actors with the intent to compromise the confidentiality, integrity, or availability of computer systems, networks, data, or personal information.

Recognizing and combating cybercrime involves identifying and preventing malicious activities carried out in the digital realm. This includes hacking, phishing, identity theft, and various forms of online fraud. As technology advances, threats and attacks will advance also. It is important that we arm ourselves with the knowledge to protect against the many cyber threats in today's world.

"There's no silver bullet solution with cyber security; a layered defense is the only viable defense".

Fun Facts!

1. FBI has reported that Cybercrimes have skyrocketed nearly 300 per cent after the Covid-19 pandemic.

2. 1 in 3 Americans suffers from at least 1 Cyber-attack every year.

3. Not all hacking is unauthorized. Most hackers fall into three general categories: black hat hackers, white hat hackers, and gray hat hackers.

4. Companies take an average of six months to detect a data breach.

Attacks and Tips!

Most Common Attacks

1. Malware
2. Denial-of-Service (DoS)
3. Phishing
4. Ransomware
5. Code Injection Attacks
6. Supply Chain Attacks
7. Insider Threats
8. IoT-Based Attacks

Tips

1. Awareness: learn how to recognize suspicious activity.
2. Install anti-virus and anti-malware software.
3. Use firewalls to monitor and filter incoming and outgoing network traffic.
4. Stay informed about current and evolving cyber threats.
5. Incident Response: have a plan in place for responding to cyber incidents and reporting to authorities if necessary.
6. Conduct regular backups.

PROTECT, DETECT, REACT!

Don’t Be a Victim