THE LIFE CYCLE OF A CYBER ATTACK...

..and when to stop it.

In accordance with:

The GenCyber program provides teachers at the K-12 level. The goals of the program are to increase interest in cybersecurity careers and diversity in the cybersecurity workforce of the nation, help all students understand correct and safe on-line behavior and how they can be good digital citizens, and improve teaching methods for delivery of cybersecurity content in K-12 curricula.

Our vision is for the GenCyber program to be part of the solution to the Nation’s shortfall of skilled cybersecurity professionals. Ensuring that enough young people are inspired to direct their talents in this area is critical to the future of our country’s national and economic security as we become even more reliant on cyber-based technology in every aspect of our daily lives.

Different Types of Attacks in 2018

Cyber Attacks happen all over the world, but what types of attacks actually occur?

Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks: A denial-of-service attack over-whelms a system’s resources so that it cannot respond to service requests.

Man-in-the-middle (MitM) attack: A MitM attack occurs when a hacker inserts itself between the communications of a client and a server.

Phishing and spear phishing attacks: Phishing attack is the practice of sending emails that appear to be from trusted sources with the goal of gaining personal information or influencing users to do something.

Drive-by attack: Drive-by download attacks are a common method of spreading malware.

Password attack: Because passwords are the most commonly used mechanism to authenticate users to an information system, obtaining passwords is a common and effective attack approach.

SQL injection attack: SQL injection has become a common issue with database-driven websites.

Cross-site scripting (XSS) attack: XSS attacks use third-party web resources to run scripts in the victim’s web browser or scriptable application.

Eavesdropping attack: Eavesdropping attacks occur through the interception of network traffic.

Birthday attack: Birthday attacks are made against hash algorithms that are used to verify the integrity of a message, software or digital signature.

Malware attack: Malicious software can be described as unwanted software that is installed in your system without your consent.


This is a live feed map showing real-time attacks occurring all over the world. Maps like these show how many attacks occur for every hour of every day. They are detailed enough to pinpoint from which country, city, and sometimes even exact addresses, different types of attacks come from. These maps also show what percentage of the type of attack (bots, malware, etc.) the attack contains or has contained. These types of tools aid in understanding cyber attacks and add to cyber threat prevention solutions.

Many threats occur all over the world and stopping these attacks is incredibly important in order to protect the privacy and the rights of human beings all over the country. Using things like live threat maps allows statisticians to create an accurate representation of the data found and create graphs or charts for visual understanding. Using this data, Cybersecurity experts are able to track and identify commonalities within certain locations and their specific attack types in order to further protect our information.

Created By: Sneha Magadi