Sharing Is Caring. If you enjoy this article, help us share with others.

Hacking started in the 1960s with phone freaking, or phreaking, which refers to using various audio frequencies to manipulate phone systems. At that time, telephone switches used various tones, or tone dialing, to indicate different functions.
Early threat actors realized that by mimicking a tone using a whistle, they could exploit the phone switches to make free long-distance calls.
In the mid-1980s, computer dial-up modems were used to connect computers to networks. Threat actors wrote “war dialling” programs that dialled each telephone number in a given area in search of computers, bulletin board systems, and fax machines.
When a phone number was found, password-cracking programs were used to gain access. Since then, general threat actor profiles and motives have changed quite a bit.
There are many different types of threat actors.

#1 Street Kiddies

Script kiddies emerged in the 1990s and refer to teenagers or inexperienced threat actors running existing scripts, tools, and exploits, to cause harm, but typically not for profit.

#2 Vulnerability Brokers

Vulnerability brokers typically refer to grey hat hackers who attempt to discover exploits and report them to vendors, sometimes for prizes or rewards.

#3 Hacktivists

Hacktivist is a term that refers to grey hat hackers who rally and protest against different political and social ideas.
Hacktivists publicly protest against organizations or governments by posting articles, videos, leaking sensitive information, and performing distributed denial of service (DDoS) attacks.

#4 Cybercriminals

Cyber criminal is a term for black hat hackers who are either self-employed or working for large cybercrime organizations.

PEOPLE ALSO READ: Unknown Facts About Marketing Automation In CRM
Powered by **Inline Related Posts**

Each year, cyber criminals are responsible for stealing billions of dollars from consumers and businesses.

#5 State-Sponsored

State-Sponsored hackers are threat actors who steal government secrets, gather intelligence, and sabotage networks of foreign governments, terrorist groups, and corporations.

Most countries in the world participate to some degree in state-sponsored hacking. Depending on a person’s perspective, these are either white hat or black hat hackers.

Cyber criminals are threat actors who are motivated to make money using any means necessary. While sometimes cybercriminals work independently, they are more often financed and sponsored by criminal organizations.
It is estimated that globally, cybercriminals steal billions of dollars from consumers and

businesses every year.
Cybercriminals operate in an underground economy where they buy, sell, and trade exploits and tools.
They also buy and sell the personal information and intellectual property that they steal from victims.
Cybercriminals target small businesses and consumers, as well as large enterprises and industries.

Cybersecurity Tasks

Threat actors do not discriminate. They target the vulnerable end devices of home users and small-to-medium-sized businesses, as well as large public and private organizations.
To make the internet and networks safer and more secure, we must all develop good cybersecurity awareness.
Cybersecurity is a shared responsibility that all users must practice.
For example, we must report cybercrime to the appropriate authorities, be aware of potential threats in email and the web, and guard important information against theft.
Organizations must take action and protect their assets, users, and customers. They must develop and practice cybersecurity tasks such as those listed in the figure.
The figure shows a cybersecurity checklist consisting of trustworthy it vender (checked),

security software up to date, regular penetration tests, backup to the cloud and hard disk, periodically change wi fi password, security policy up to date, enforce the use of strong passwords, and two-factor authentication.

Cyber Threat Indicators

Many network attacks can be prevented by sharing information about **indicators of compromise** (IOC).

Each attack has unique identifiable attributes. Indicators of compromise are the evidence that an attack has occurred. IOCs can be features that identify malware files, IP addresses of servers that are used in attacks, filenames, and characteristic changes made to end system software, among others.

IOCs help cybersecurity personnel identify what has happened in an attack and develop defences against the attack. A summary of the IOC for a piece of malware is shown in the figure

For instance, a user receives an email claiming they have won a big prize. Clicking on the link in the email results in an attack.

The IOC could include the fact the user did not enter that contest, the IP address of the sender, the email subject line, the URL to click, or an attachment to download, among others.

Indicators of attack (IOA) focus more on the motivation behind an attack and the potential means by which threat actors have, or will, compromise vulnerabilities to gain access to assets.

IOAs are concerned with the strategies that are used by attackers. For this reason, rather than informing response to a single threat, IOAs can help generate a proactive security approach.

This is because strategies can be reused in multiple contexts and multiple attacks. Defending against a strategy can therefore prevent future attacks that utilize the same, or similar strategy.

Action Point

PS: I know you might agree with some of the points raised in this article or disagree with some of the issues raised.

Please share your thoughts on the topic discussed. We would appreciate it if you could drop your comment. Thanks in anticipation.

Sharing Is Caring. If you enjoy this article, help us share with others.

PEOPLE ALSO READ: Customer Care In CRM: How To Retain Customers For Life (+Examples)

Powered by **Inline Related Posts**

Related posts:

1. Overview Of Customer Relationship Management
2. Customer Centricity In CRM: What You Should Know (+Examples)
3. Customer-Centric Strategy In CRM: What You Should Know (+Examples)
4. Internet And CRM: The Relationships And Differences (+Examples)