Global Certificate in Cyber Psychology

Cybercrime and Psychology

Account Takeover: A type of cybercrime where a malicious actor gains unauthorized access to a victim's online account, such as email, social media, or banking, with the intent to steal personal information, make fraudulent purchases, or spread malware.

Advanced Persistent Threat (APT): A stealthy and sophisticated cyber threat, typically carried out by a well-resourced and trained group, aimed at obtaining access to sensitive information or intellectual property over an extended period.

Anti-virus (AV) Software: Software designed to detect, prevent, and remove malicious software (malware) from a computer system. AV software uses various techniques to identify known malware signatures, heuristics, and behavior-based analysis.

Artificial Intelligence (AI): The simulation of human intelligence in machines that are programmed to think and learn like humans, including problem-solving, pattern recognition, and decision-making. AI has applications in cybersecurity, including intrusion detection and prevention, and phishing detection.

Behavioral Analytics: The use of data analytics and machine learning to identify patterns of behavior in user activity, network traffic, and other data sources to detect anomalies and potential cyber threats.

Black Hat Hacker: A malicious hacker who uses their skills to exploit vulnerabilities in computer systems, steal sensitive information, or cause damage to systems or networks.

Bot: A type of malware that enables a malicious actor to take control of a victim's computer or device and use it to carry out automated tasks, such as sending spam emails, participating in DDoS attacks, or stealing sensitive information.

Brute Force Attack: A method of attempting to gain unauthorized access to a system or network by trying multiple combinations of usernames, passwords, or other authentication factors until the correct one is found.

Computer Forensics: The process of collecting, analyzing, and preserving digital evidence in a way that is admissible in court. Computer forensics is used in investigations of cybercrime, intellectual property theft, and other digital crimes.

Cybersecurity Framework: A set of guidelines and best practices for managing cybersecurity risks, developed by organizations such as the National Institute of Standards and Technology (NIST) or the Center for Internet Security (CIS).

Data Breach: An incident in which sensitive or confidential information is accessed, stolen, or disclosed without authorization, often as a result of a cyber attack or other security vulnerability.

Dark Web: A part of the internet that is not indexed by search engines and is accessible only through specialized software, such as the Tor browser. The dark web is often associated with illegal activities, such as the sale of drugs, weapons, and stolen data.

Denial of Service (DoS) Attack: A type of cyber attack that floods a network or system with traffic, overwhelming its resources and preventing legitimate users from accessing it.

Distributed Denial of Service (DDoS) Attack: A type of DoS attack that uses multiple compromised devices, such as botnets, to flood a network or system with traffic, making it even more difficult to defend against.

Email Phishing: A type of social engineering attack that uses email to trick victims into revealing sensitive information, such as passwords or credit card numbers, or installing malware on their devices.

End-user Education: The process of educating and training users on cybersecurity best practices, such as creating strong passwords, recognizing phishing emails, and avoiding risky behaviors that can compromise security.

Encryption: The process of converting plain text into a coded format that is difficult to decipher without the correct key, used to protect sensitive information in transit or at rest.

Firewall: A security device or software that monitors and controls incoming and outgoing network traffic based on predefined rules, used to prevent unauthorized access to a network or system.

Hacker: A person who uses their technical skills to gain unauthorized access to a system or network, often for malicious purposes, but sometimes for legitimate security testing or research.

Heuristics: A set of rules or algorithms used by security software to identify and analyze previously unknown or zero-day threats, based on patterns of behavior or other indicators.

Incident Response: The process of identifying, investigating, and mitigating a security incident, such as a data breach or cyber attack, to minimize damage and prevent future occurrences.

Insider Threat: A security risk posed by employees, contractors, or other authorized users who have access to a system or network and use that access for malicious purposes, such as data theft or sabotage.

Intrusion Detection System (IDS): A security device or software that monitors network traffic and alerts security personnel when suspicious or malicious activity is detected.

Malware: Short for "malicious software," malware is any software designed to harm a computer system, steal sensitive information, or disrupt normal operations. Examples of malware include viruses, worms, Trojans, and ransomware.

Penetration Testing: The process of testing a system or network for vulnerabilities by simulating attacks, often performed by ethical hackers or security researchers to identify weaknesses and recommend remediation.

Phishing: A type of social engineering attack that uses email, text messages, or other communication

channels to trick victims into revealing sensitive information or installing malware on their devices.

Ransomware: A type of malware that encrypts a victim's files or entire system and demands payment in exchange for the decryption key, often used for financial gain or to disrupt operations.

Risk Assessment: The process of identifying and evaluating potential security risks and vulnerabilities, often performed as part of a larger cybersecurity strategy or compliance requirement.

Social Engineering: The use of psychological manipulation to trick users into revealing sensitive information or performing actions that compromise security, often through phishing emails, phone calls, or other communication channels.

Two-Factor Authentication (2FA): A security measure that requires users to provide two forms of authentication, such as a password and a one-time code sent to their mobile device, to access a system or network.

Virus: A type of malware that infects a victim's device and replicates itself, often by attaching itself to other files or programs, used to steal sensitive information, disrupt operations, or spread spam or other malware.

Vulnerability: A weakness or flaw in a system or network that can be exploited by attackers to gain unauthorized access, steal sensitive information, or disrupt operations.

Whitelisting: A security measure that allows only authorized software or devices to access a system or network, often used to prevent malware or unauthorized access.

Worm: A type of malware that replicates itself and spreads from device to device without requiring user interaction, often used to spread spam or other malware.

Zero-Day Exploit: A previously unknown vulnerability in a system or network that is exploited by attackers before a patch or other remediation is available, often used in advanced persistent threats (APTs) or other sophisticated attacks.

Zero-Day Malware: Malware that exploits a previously unknown vulnerability, making it difficult to detect and remediate, often used in advanced persistent threats (APTs) or other sophisticated attacks.