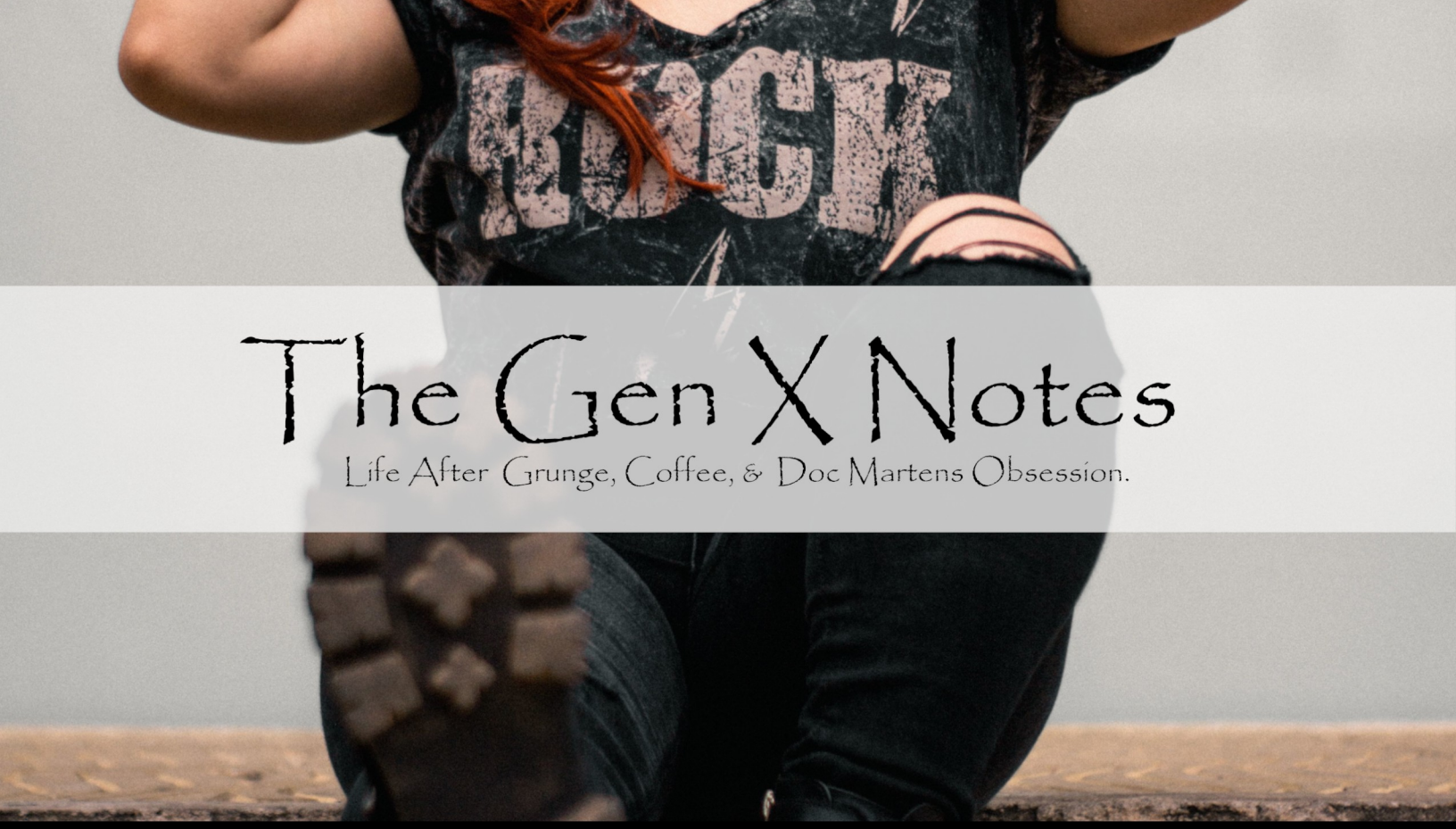


The Gen X Notes

Life After Grunge, Coffee, & Doc Martens Obsession.

SHADOW ACTORS

How Cybercriminals Gain Access



Five common ways threat actors access sensitive, confidential personal or organizational data.

Copyright-Free

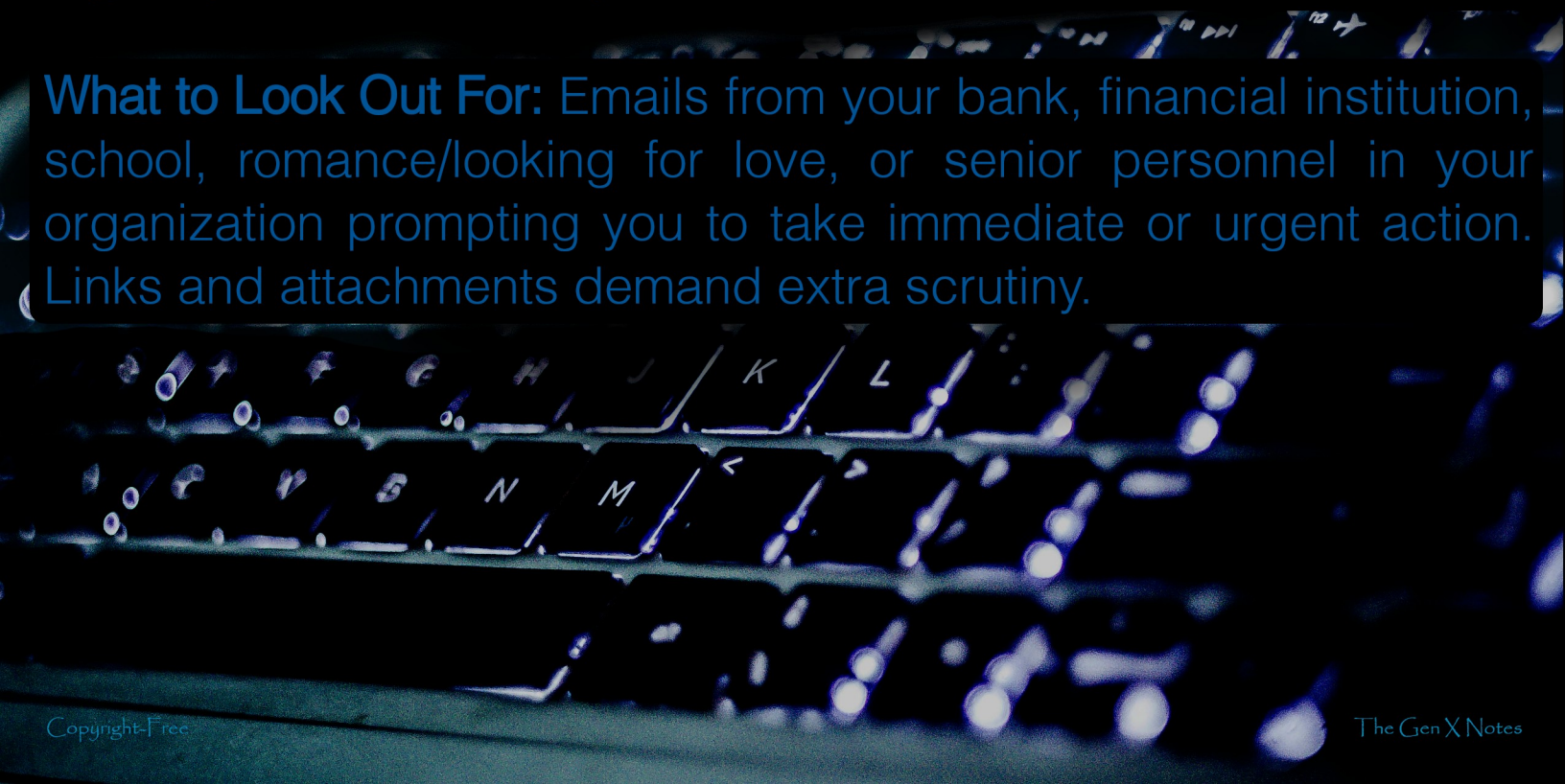
SHADOW ACTORS

How Cybercriminals Gain Access

Cyber threat actors employ a variety of techniques to harvest passwords, breach systems, infect devices, and hijack networks. Be mindful of these five common ways they could obtain access to your personal information or organizational data.

Social Engineering Attacks: A social engineering attack is when a threat actor—pretending to be someone you know or trust—uses psychological coercion or manipulation to get you to share sensitive, confidential information or perform actions that compromise security. Common types of social engineering attacks include phishing, whaling, pretexting, piggybacking, and honeytraps—gateways to larger cyberattacks. The communication appears legitimate and creates a strong sense of urgency, fear, or curiosity.

What to Look Out For: Emails from your bank, financial institution, school, romance/looking for love, or senior personnel in your organization prompting you to take immediate or urgent action. Links and attachments demand extra scrutiny.



Copyright-Free

SHADOW ACTORS

How Cybercriminals Gain Access

Malware: Malware is malicious software designed to harm, disrupt, or take control of devices and data. Threat actors use malware to steal information, encrypt or delete files, spy on network activities, or hijack system functions.

What to Look Out For: Signs of infection include slow performance, pop-ups, frequent crashes, unusual network activity, or altered settings. Malware spreads mainly through hacked sites, malicious downloads, risky apps, and phishing emails. Social Engineering attacks are a common vector for malware transmission. Examples include adware, spyware, viruses, exploits, Trojans, ransomware, rootkits, and keyloggers.



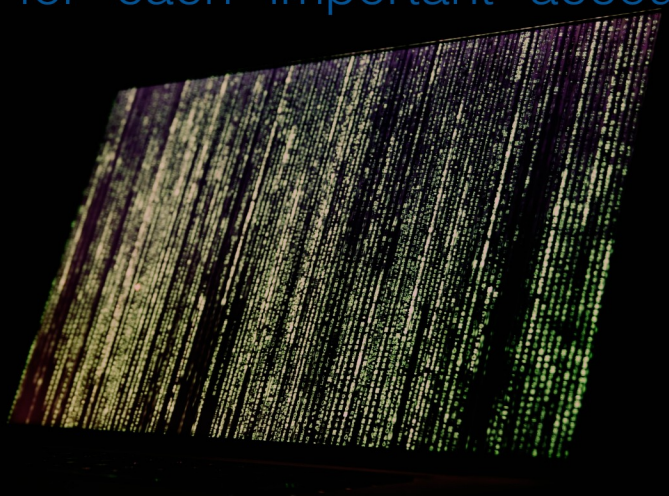
Copyright-Free

SHADOW ACTORS

How Cybercriminals Gain Access

Brute Force Attacks: A cyberattack in which a threat actor tries many possible passwords or encryption keys through trial and error until the correct one works. It can last hours and target login systems (like website logins, SSH, or password-protected files). The five types of brute force attacks are: Simple Brute Force Attack, Dictionary Attacks, Hybrid Brute Force Attack, Credential Stuffing, and Reverse Brute Force Attacks. Strong passwords, MFA, 2FA, and proper protections make it much harder or impractical. Weak passwords are especially vulnerable to this method.

What to Look Out For (Defense): Use strong, multi-character passwords; avoid “dictionary” words; avoid passwords that may be easy to guess (birthday, graduation date, favorite anything), change your password every six months or so and, if possible, use a unique password for each important account; use a password manager.

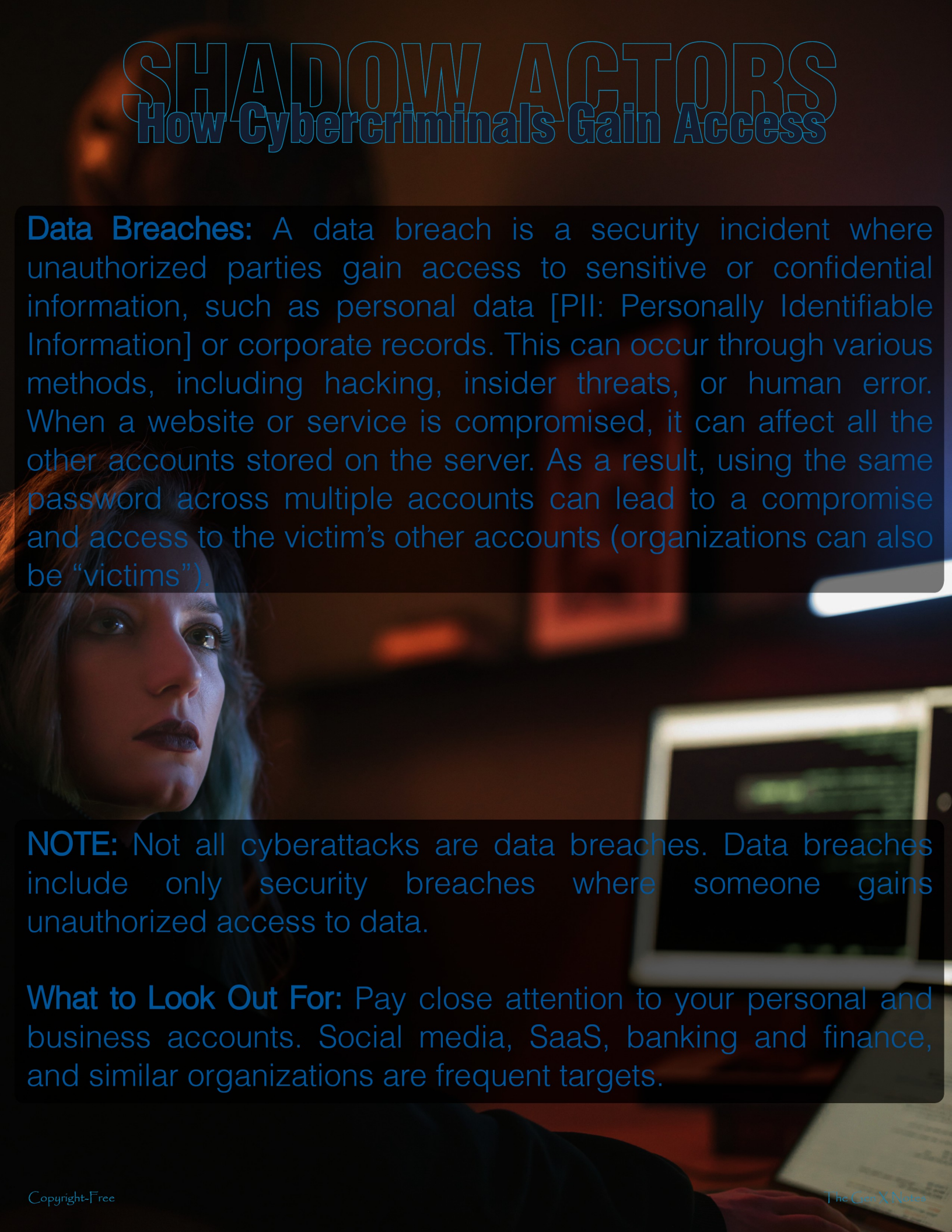


Copyright-Free

SHADOW ACTORS

How Cybercriminals Gain Access

Data Breaches: A data breach is a security incident where unauthorized parties gain access to sensitive or confidential information, such as personal data [PII: Personally Identifiable Information] or corporate records. This can occur through various methods, including hacking, insider threats, or human error. When a website or service is compromised, it can affect all the other accounts stored on the server. As a result, using the same password across multiple accounts can lead to a compromise and access to the victim's other accounts (organizations can also be "victims").



NOTE: Not all cyberattacks are data breaches. Data breaches include only security breaches where someone gains unauthorized access to data.

What to Look Out For: Pay close attention to your personal and business accounts. Social media, SaaS, banking and finance, and similar organizations are frequent targets.

Copyright-Free

SHADOW ACTORS

How Cybercriminals Gain Access

Cyber threat actors employ a variety of techniques to harvest passwords, breach systems, infect devices, and hijack networks. This includes...

Credentials Sale & Bartering: Cybercriminals can buy, sell, and trade your credentials, passwords, and other data online, often on the Dark Web. Cybercriminals are experts in stealing, storing, and selling victims' credentials to other cybercriminals.



Copyright-Free

SHADOW ACTORS

How Cybercriminals Gain Access

GLOSSARY

Dictionary Attack: A password-cracking method where an attacker uses a prewritten list of common passwords or "words" (called a dictionary) and systematically tries them against the target. The dictionary may contain words from an English language dictionary, or a leaked list of commonly used passwords. Combined with common character replacement using numbers, the tactic can be fast and highly effective.

Honeytrap: A social engineering tactic that specifically targets individuals seeking love in digital spaces. The cybercriminal befriends the victim by creating a fictional persona and setting up a fake online profile. Over time, the criminal abuses the relationship and tricks the victim into giving them money, extracting personal information, or installing malware.

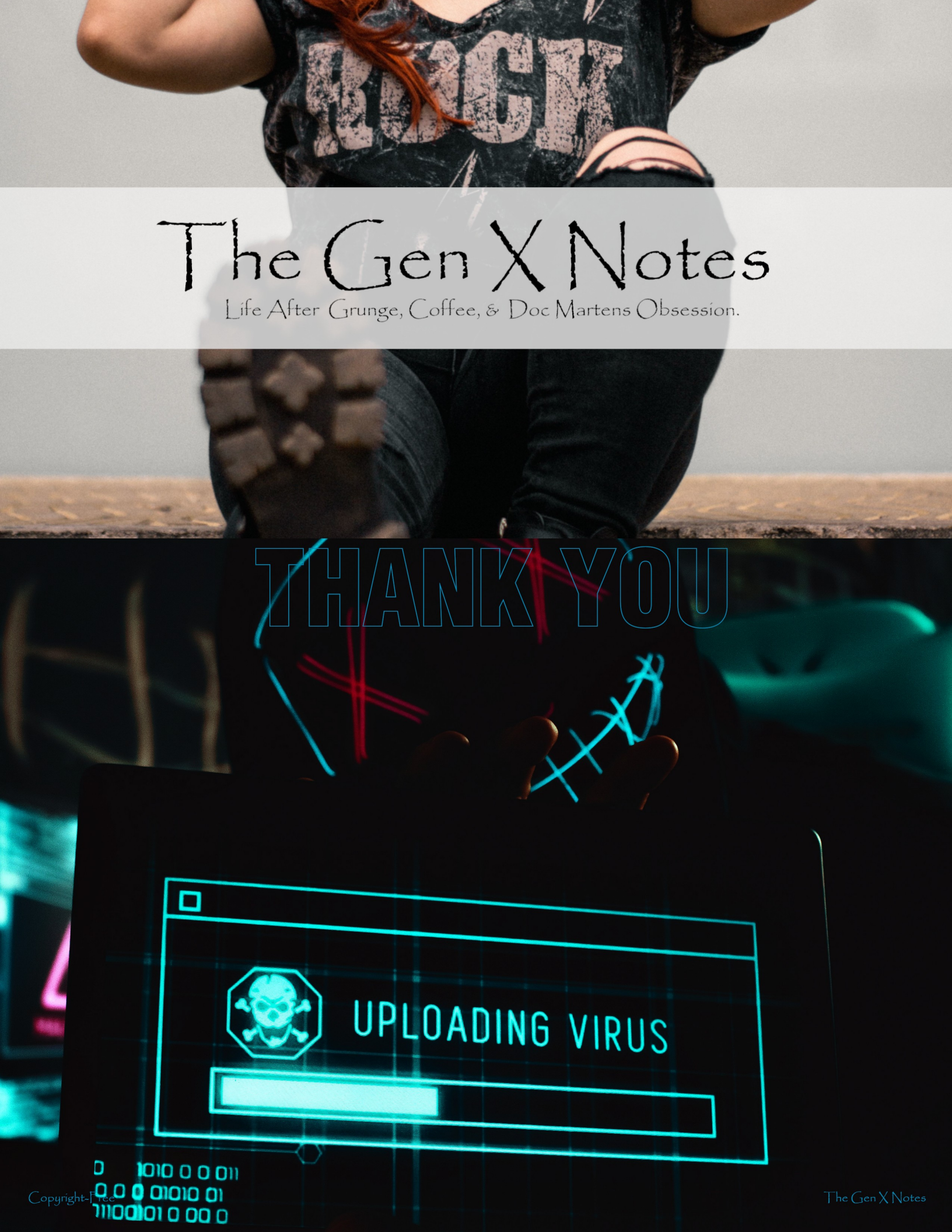
Phishintg: A cyberattack that takes advantage of email, phone, SMS, social media, or other forms of communication to lure users into clicking a malicious link, downloading infected files, or revealing Personally Identifiable Information (PII), such as passwords or account numbers. Cybercriminals may pretend to be retailers, service providers, or government agencies to extract seemingly harmless personal data such as email addresses, phone numbers, the user's date of birth, or the names of family members. A social engineering tactic, it preys on users' vulnerabilities and gullibility.

Piggybacking/Tailgating: A physical security breach. The threat actor gains access to a physical facility by asking the person entering ahead of them to hold the door or, under the guise of forgetting their ID, grant them access. The actor may impersonate a delivery driver or other plausible identity to increase their chances. Once inside the facility, the criminal can use their time to conduct reconnaissance, steal unattended devices, or access confidential files. Tailgating can also occur when an unauthorized person borrows an employee's laptop or other device, then installs malware.

Pretexting: A social engineering tactic that involves composing plausible scenarios, "pretext," that are likely to convince victims to share valuable and sensitive data. Pretexters often impersonate someone in a position of authority, such as a law enforcement or tax official, or a person of interest, such as a talent scout or sweepstakes organizer. After providing context, the attacker questions the victim, hoping to gain access to personal and sensitive information. The information obtained is then used to advance other attack scenarios or access the victim's personal accounts.

Whaling: A type of phishing attack that targets "big game," hence the name. This tactic also leverages personal communication to access a user's device or personal information. While phishing attacks are not personalized and can be replicated for millions of users, whaling attacks target a single individual. Typically, this is a high-level executive. This type of attack requires sophistication and significant research to be successful. The intent is to access high-value data or the financial resources needed to advance a ransomware attack.

Copyright-Free



Copyright-Free