Stealing of passwords

Have you wondered how hackers steal passwords? Unfortunately, we make it easy for them with weak passwords that are simple to crack. By simply taking advantage of low hanging account passwords, hackers steal the most sensitive data to perform blackmailing, identity fraud, extortion, and other illegal activities. The hacking of a user's password might even be worse than personally identifiable information (PII) as it exposes the user's online accounts. Email is often used to verify passwords and store information of other accounts, and a stolen email account password can lead to more cases of scam and identity theft.

Here's how Hackers Steal Your Passwords

According to recent studies on data and identity theft, various small to medium-sized businesses (SMBs) still believe that they are saved from hackers stealing passwords. Many believe their businesses don't have as much precious data as larger companies and hackers won't attack them. The following are the ways hackers steal passwords from an individual to an organization of all sizes.

Brute force attack:

Brute force attacks are trial and error sessions done various times per minute using a specific program and your private information or words that may value to you.

It's not all random words or information. Some extra advanced brute force hacking codes and programs use further targeted words that are possible to be used as passwords. These words are prioritized to make passwords with a greater possibility of matching.

Spidering:

This password-stealing technique gathers information from company sites or social media websites like Instagram or Twitter to come up with word lists, which are then used to conduct brute force and dictionary attacks on the users.

Rainbow table attacks:

Though it sounds like a board game, this kind of attack deals with hashes i.e., the encrypted values of passwords. The rainbow table includes pre-computed hashes of password parts that, when rightly joined, provide the full hash of the target's real password. While the more professional approach of this attack could produce quicker results, it could also take up a lot of computing power to operate.

Phishing:

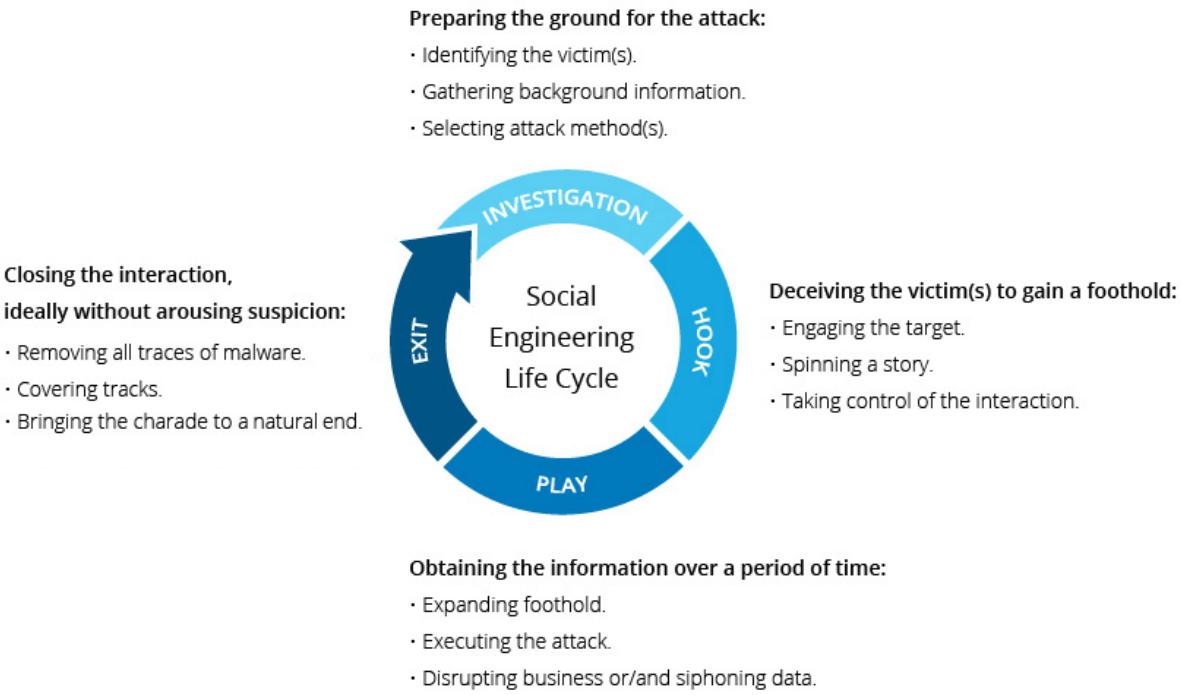
Phishing is one of the most common and regularly used password hacks. A hacker will send an email that carries a link that, once clicked, guides to a spoofed website that encourages the person to give their password or other information. In other scenarios, the hacker tries to trick the user to download a malicious program that skims for the user's password.

Social engineering:

According to Hacker's point of view, if all else fails, use the simplest trick in the book and do it the traditional way. Social engineering is the use of psychological manipulation to gain the trust of an unwitting user. For example, a hacker could drop a harmless thumb drive in an office. Shortly as a victim installs it (normally to obtain information that can help recognize and find its owner), the device will load malware onto the system to steal passwords.

Social engineering

Social engineering is a non-technical strategy that cyber attacker use that relies heavily on human interaction and often involves tricking people into breaking standard security practices. The success of social engineering techniques depends on attackers' ability to manipulate victims into performing certain actions or providing confidential information. Today, social engineering is recognized as one of the greatest security threats facing organizations. Social engineering differs from traditional hacking in the sense that social engineering attacks can be non-technical and don't necessarily involve the compromise or exploitation of software or systems. When successful, many social engineering attacks enable attackers to gain legitimate, authorized access to confidential information.



What makes social engineering especially dangerous is that it relies on human error, rather than vulnerabilities in software and operating systems. Mistakes made by legitimate users are much less predictable, making them harder to identify and thwart than a malware-based intrusion.

Here is a breakdown of common social engineering techniques:

- Baiting – Attackers conduct baiting attacks when they leave a malware-infected device, such as a USB flash drive or CD, in a place where someone likely will find it. The success of a baiting attack hinges on the notion that the person who finds the device will load it into their computer and unknowingly install the malware. Once installed, the malware allows the attacker to advance into the victim's system.
- Phishing – Phishing occurs when an attacker makes fraudulent communications with a victim that are disguised as legitimate, often claiming or seeming to be from a trusted source. In a phishing

attack the recipient is tricked into installing malware on their device or sharing personal, financial, or business information. Email is the most popular mode of communication for phishing attacks, but phishing may also utilize chat applications, social media, phone calls, or spoofed websites designed to look legitimate. Some of the worst phishing attacks make charity pleas after natural disasters or tragedies strike, exploiting people's goodwill and urging them to donate to a cause by inputting personal or payment information.

- Pretexting – Pretexting occurs when an attacker fabricates false circumstances to compel a victim into providing access to sensitive data or protected systems. Examples of pretexting attacks include a scammer pretending to need financial data in order to confirm the identity of the recipient or masquerading as a trusted entity such as a member of the company's IT department in order to trick the victim into divulging login credentials or granting computer access.
- Quid pro quo – A quid pro quo attack occurs when attackers request private information from someone in exchange for something desirable or some type of compensation. For instance, an attacker requests login credentials in exchange for a free gift. Remember, if it sounds too good to be true, it probably is.
- Spear phishing – Spear phishing is a highly targeted type of phishing attack that focuses on a specific individual or organization. Spear phishing attacks use personal information that is specific to the recipient in order gain trust and appear more legitimate. Often times this information is taken from victims' social media accounts or other online activity. By personalizing their phishing tactics, spear phishers have higher success rates for tricking victims into granting access or divulging sensitive information such as financial data or trade secrets.
- Tailgating – Tailgating is a physical social engineering technique that occurs when unauthorized individuals follow authorized individuals into an otherwise secure location. The goal of tailgating is to obtain valuable property or confidential information. Tailgating could occur when someone asks you to hold the door open because they forgot their access card or asks to borrow your phone or laptop to complete a simple task and instead installs malware or steals data.

Social engineering prevention:

- Don't open emails and attachments from suspicious sources – If you don't know the sender in question, you don't need to answer an email. Even if you do know them and are suspicious about their message, cross-check and confirm the news from other sources, such as via telephone or directly from a service provider's site. Remember that email addresses are spoofed all of the time; even an email purportedly coming from a trusted source may have actually been initiated by an attacker.
- Use multifactor authentication – One of the most valuable pieces of information attackers seek are user credentials. Using multifactor authentication helps ensure your account's protection in the event of system compromise. Imperva Login Protect is an easy-to-deploy 2FA solution that can increase account security for your applications.
- Be wary of tempting offers – If an offer sounds too enticing, think twice before accepting it as fact. Googling the topic can help you quickly determine whether you're dealing with a legitimate offer or a trap.
- Keep your antivirus/antimalware software updated – Make sure automatic updates are engaged, or make it a habit to download the latest signatures first thing each day. Periodically check to make sure that the updates have been applied, and scan your system for possible infections.

Bugs

An unintended flaw in software code or in system is called a bug. That leaves your system open to the potential for exploitation in the form of unauthorized access or malicious behavior such as viruses, worms, Trojan horses and other forms of malware.

Backdoors

In the world of cybersecurity, **a backdoor refers to any method by which authorized and unauthorized users are able to get around normal security measures and gain high level user access on a computer system, network, or software application.** Once they're in, cybercriminals can use a backdoor to steal personal and financial data, install additional malware, and hijack devices. But backdoors aren't just for bad guys. Backdoors can also be installed by software or hardware makers as a deliberate means of gaining access to their technology after the fact. Backdoors of the non-criminal variety are useful for helping customers who are hopelessly locked out of their devices or for troubleshooting and resolving software issues.

A backdoor is a malware type that negates normal authentication procedures to access a system. As a result, remote access is granted to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware. Backdoor installation is achieved by taking advantage of vulnerable components in a web application. Once installed, detection is difficult as files tend to be highly obfuscated.

Webserver backdoors are used for a number of malicious activities, including:

- Data theft
- Website defacing
- Server hijacking
- The launching of distributed denial of service (DDoS) attacks
- Infecting website visitors (watering hole attacks)

AUTHENTICATION FAILURE

This error message indicates that the authentication process between your local computer and the remote host computer has failed.
Possible reasons:

- The most common cause for failed authentication is an incorrect password, likely caused by a typing mistake.
- The user name may be incorrect. Check that you have typed it correctly.
- One possible reason for authentication failure is that the remote host computer may have been configured to require several authentication methods to be used. For example, both password and public-key authentication could be used for increased security. Even if you entered your password correctly, another required authentication method could have failed. A relatively common situation is one where the remote host computer is expecting public-key authentication and you have not sent your public key to the host. You can do this by following the instructions in Section Uploading Your Public Key.
- It is also possible that your account on the remote host computer has been disabled, or that the remote host computer is having temporary problems that cause errors with the login procedure.

Try to connect again and carefully type in your user name and password. If after a couple of retries you are sure that you have entered both of them correctly, contact the system administrator of the remote host computer.

Protocol Failures

In cryptosystems where the message is first converted to numbers which are then acted on, there are several pitfalls which need to be avoided. These are collectively known as *protocol failures* since they are not weaknesses of the cryptosystem, but rather of the way the system is implemented.

Dictionary Attacks

A dictionary attack on a cryptosystem occurs when it is possible to take all the components that are used to make up a plaintext and encrypt them separately (as in taking all the words in a dictionary and finding their encrypted equivalents). To decrypt a message given such a list, one only has to do a table look up to find the corresponding plaintext. Thus, for example, if in a public key system based on factoring (such as RSA) or the discrete log problem, the plaintext message is blocked into blocks of size one (i.e., individual letters) which are then run through the encryption algorithm, the cryptanalyst has an easy method for decrypting without finding the key.

Example: The plaintext was encoded by replacing each letter with its corresponding value mod 26, i.e., A = 0, B = 1, C = 2 , etc. The RSA system was used to encipher this message using the public values n = 18721 and encryption exponent 25, and the following ciphertext was produced: 365, 0, 4845, 14930, 2608, 2608, 0

The cryptanalyst, knowing this encoding scheme, just calculates x25 mod (18721) for each x in the range 0 to 25 to get the following table of values:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	6400	18718	17173	1759	18242	12359	14930	9	6279	2608	4644
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4845	1375	13444	16	13663	1437	2940	10334	365	10789	8945	11373	5116

The plaintext message can then be read off from the table : VANILLA.

To avoid this pitfall, the blocks of the message must be long enough so that it is impractical to store all possible blocks and their encrypted equivalents.