REVALSYS
CREATING POSSIBILITIES

COMMON TYPES OF PASSWORD ATTACKS
AND TIPS FOR PREVENTING THEM

Article from Revalsys Technologies

This article explains about the common types of password attacks and tips for preventing them

A password attack is exactly that – it is where a hacker tries to steal his victim's password. Stolen passwords are a common cause of data breaches. Around 579 passwords are hacked per second. Password attacks are easy to carry out because most people and businesses do not have the necessary security measures in place to protect themselves from these attacks.

On a personal level, password attacks cause a leakage of sensitive personal information. On an organizational level, these attacks result in business downtime, leakage of confidential financial information, a loss of reputation, and in turn, customers.

Passwords may seem like a small element of online accounts, but they are an important aspect of cybersecurity. To avoid falling prey to password attacks, you must first understand how hackers obtain your passwords. Following are some of the most common types of password attacks that you must beware of along with tips to prevent them:

Phishing Attack

Phishing is the most common kind of cyberattack today. It is carried out through the medium of email and its victims easily fall for it as fraudsters impersonate their family members, friends, colleagues, or reputed brands. Fraudsters include malicious links in their emails that take victims to fake login pages and force them to log into them under the pretext of changing expired passwords. Once the victim clicks on the malicious link and enters their login details, the hacker uses those details to hack into that account as well as into other accounts that share the same password.

Knowing what a phishing email looks like can help you to avoid clicking on it. There are a few signs you must look out for which indicate that an email you received is a phishing email:

- The address of the email does not look right
- The email's sender is unknown to you
- There are grammatical errors in the subject and the body copy of the email

Man-In-The-Middle Attack

A man-in-the-middle attack is one where the hacker is in the middle of two systems, pretending to be both the parties. The hacker intercepts, decrypts, and re-encrypts the data that is being exchanged between the two systems, including passwords. This information can be used by the hacker to send malicious links to either party, carry out illegal transactions, or change the passwords.

You can protect your accounts from man-in-the-middle attacks by securing your Wi-Fi router with encryption, using an HTTPS URL or a VPN (Virtual Private Network), and securing your accounts with two-factor authentication which involves using two different methods to log into accounts.

Brute Force Attack

One of the easiest and most commonly used password attack techniques, a brute force attack uses a trial-and-error method to guess a system's password. Using software hackers try multiple possible character combinations until they get the password right. Hackers start with easy-to-guess and most used passwords, so this attack puts passwords like "password", "qwerty", and "1234567" at risk.

Brute force attacks can be delayed by limiting the number of allowed log-in attempts and by using longer, strong passwords which are a combination of alphabets, numbers, and special characters.

Dictionary Attack

A dictionary attack is a type of brute force attack. The difference between the two is that a dictionary attack uses words that can be found in dictionaries as guesses instead of different combinations of alphabets and numbers. It is a targeted form of attack that uses words that are commonly used by individuals and organizations, like nicknames of people and names of services respectively.

You can avert a dictionary attack by avoiding using words that are personal to you as passwords. Although using this technique makes your passwords easy to remember for you, it also makes them easy for hackers to guess. You should also be wary of sharing personal information online.

Credential Stuffing

Credential stuffing takes advantage of accounts whose passwords have not been changed in a long time. Attackers create a database of such passwords and use one of them to log in to multiple other accounts and compromise their data.

You can avoid falling prey to credential stuffing by following good password hygiene. The longer a password remains unchanged, the more amount of time a hacker gets to guess it, and the higher are its chances of getting hacked. It is recommended that you use phrases instead of words as passwords as the latter are easy to guess. Keep changing passwords every 3-6 months, avoid noting them down on papers or emailing them, and store them in a safe place.

Keylogger Attack

A keylogger is a spyware that a hacker installs in the system of his victim. Using this spyware, the hacker tracks every single stroke of the victim's keyboard without his knowledge to steal his passwords. A keylogger is also installed in the form of hardware, but it is less common as its installation is hard.

Keylogger attacks can be prevented by using multifactor authentication, regularly updating passwords and checking for bugs and updating applications and software with the latest security patches.

CONTACTS

For more information on Revalsys Technologies, visit www.revalsys.com

8-2-293/82/1/83-A, 1st Floor,
Road No 12, Banjara Hills,
MLA Colony,
Hyderabad - 500034
Telangana, India

Phone: +91 7032660301

info@revalsys.com