UNIT 1.5

Common Password Attacks

Six Types of Password Attacks & How to Stop Them

Password attacks are one of the most common forms of corporate and personal data breach. A password attack is simply when a hacker trys to steal your password. In 2020, 81% of data breaches were due to compromised credentials. Because passwords can only contain so many letters and numbers, passwords are becoming less safe. Hackers know that many passwords are poorly designed, so password attacks will remain a method of attack as long as passwords are being used.

Protect yourself from password attacks with the information below.

1. Phishing

Phishing is when a hacker posing as a trustworthy party sends you a fraudulent email, hoping you will reveal your personal information voluntarily. Sometimes they lead you to fake “reset your password” screens; other times, the links install malicious code on your device. We highlight several examples on the OneLogin blog.

Here are a few examples of phishing:

Regular phishing. You get an email from what looks like goodwebsite.com asking you to reset your password, but you didn’t read closely and it’s actually goodwobsite.com. You “reset your password” and the hacker steals your credentials.

Spear phishing. A hacker targets you specifically with an email that appears to be from a friend, colleague, or associate. It has a brief, generic blurb (“Check out the invoice I attached and let me know if it makes sense.”) and hopes you click on the malicious attachment.

Smishing and vishing. You receive a text message (SMS phishing, or smishing) or phone call (voice phishing, or vishing) from a hacker who informs you that your account has been frozen or that fraud has been detected. You enter your account information and the hacker steals it.

Whaling. You or your organization receive an email purportedly from a senior figure in your company. You don’t do your homework on the email’s veracity and send sensitive information to a hacker.

To avoid phishing attacks, follow these steps:

Check who sent the email: look at the From: line in every email to ensure that the person they claim to be matches the email address you’re expecting.

Double check with the source: when in doubt, contact the person who the email is from and ensure that they were the sender.

Check in with your IT team: your organization's IT department can often tell you if the email you received is legitimate.

1. **Man in the Middle Attack**

Man-in-the middle (MitM) attacks are when a hacker or compromised system sits in between two uncompromised people or systems and deciphers the information they're passing to each other, including passwords. If Alice and Bob are passing notes in class, but Jeremy has to relay those notes, Jeremy has the opportunity to be the man in the middle. Similarly, in 2017, Equifax removed its apps from the App Store and Google Play store because they were passing sensitive data over insecure channels where hackers could have stolen customer information.

To help prevent man-in-the-middle attacks:

Enable encryption on your router. If your modem and router can be accessed by anyone off the street, they can use "sniffer" technology to see the information that is passed through it.

Use strong credentials and two-factor authentication. Many router credentials are never changed from the default username and password. If a hacker gets access to your router administration, they can redirect all your traffic to their hacked servers.

Use a VPN. A secure virtual private network (VPN) will help prevent man-in-the-middle attacks by ensuring that all the servers you send data to are trusted.

2. **Brute Force Attack**

If a password is equivalent to using a key to open a door, a brute force attack is using a battering ram. A hacker can try 2.18 trillion password/username combinations in 22 seconds, and if your password is simple, your account could be in the crosshairs.

To help prevent brute force attacks:

Use a complex password. The difference between an all-lowercase, all-alphabetic, six-digit password and a mixed case, mixed-character, ten-digit password is enormous. As your password's complexity increases, the chance of a successful brute force attack decreases.

Enable and configure remote access. Ask your IT department if your company uses remote access management. An access management tool like OneLogin will mitigate the risk of a brute-force attack.

Require multi-factor authentication. If multi-factor authentication (MFA) is enabled on your account, a potential hacker can only send a request to your second factor for access to your account. Hackers likely

won't have access to your mobile device or thumbprint, which means they'll be locked out of your account.

3. **Dictionary Attack**

A type of brute force attack, dictionary attacks rely on our habit of picking "basic" words as our password, the most common of which hackers have collated into "cracking dictionaries." More sophisticated dictionary attacks incorporate words that are personally important to you, like a birthplace, child's name, or pet's name.

To help prevent a dictionary attack:

Never use a dictionary word as a password. If you've read it in a book, it should never be part of your password. If you must use a password instead of an access management tool, consider using a password management system.

Lock accounts after too many password failures. It can be frustrating to be locked out of your account when you briefly forget a password, but the alternative is often account insecurity. Give yourself five or fewer tries before your application tells you to cool down.

Consider investing in a password manager. Password managers automatically generate complex passwords that help prevent dictionary attacks.

4. **Credential Stuffing**

If you've suffered a hack in the past, you know that your old passwords were likely leaked onto a disreputable website. Credential stuffing takes advantage of accounts that never had their passwords changed after an account break-in. Hackers will try various combinations of former usernames and passwords, hoping the victim never changed them.

To help prevent credential stuffing:

Monitor your accounts. There are paid services that will monitor your online identities, but you can also use free services like haveIbeenpwned.com to check whether your email address is connected to any recent leaks.

Regularly change your passwords. The longer one password goes unchanged, the more likely it is that a hacker will find a way to crack it.

Use a password manager. Like a dictionary attack, many credential stuffing attacks can be avoided by having a strong and secure password. A password manager helps maintain those.

5. **Keyloggers**

Keyloggers are a type of malicious software designed to track every keystroke and report it back to a hacker. Typically, a user will download the software believing it to be legitimate, only for it to install a keylogger without notice.

To protect yourself from keyloggers:

Check your physical hardware. If someone has access to your workstation, they can install a hardware keylogger to collect information about your keystrokes. Regularly inspect your computer and the surrounding area to make sure you know each piece of hardware.

Run a virus scan. Use a reputable antivirus software to scan your computer on a regular basis. Antivirus companies keep their records of the most common malware keyloggers and will flag them as dangerous.

Preventing Password Attacks

The best way to fix a password attack is to avoid one in the first place. Ask your IT professional about proactively investing in a common security policy that includes:

Multi-factor authentication. Using a physical token (like a Yubikey) or a personal device (like a mobile phone) to authenticate users ensures that passwords are not the sole gate to access.

Remote access. Using a smart remote access platform like OneLogin means that individual websites are no longer the source of user trust. Instead, OneLogin ensures that the user's identity is confirmed, then logs them in.

Biometrics. A malicious actor will find it very difficult to replicate your fingerprint or facial shape. Enabling biometric authentication turns your password into only one of several points of trust that a hacker needs to overcome.