Metatitle: Types of password attack and how to prevent them
Meta descritpion: The new hybrid work environment introduced plenty more opportunities for hackers to attack your workforce via password vulnerabilities. Discover the types of password attacks, and how you can protect yourself against them.

What are the types of password attacks and how can you prevent them?

Traditional authentication using a username and password has been the foundation of digital identity and security for over 50 years. However, as organisations rely on a greater number of tools and applications, they face a greater risk of password attack.

According to our latest Businesses at Work report, the average number of corporate and personal apps organisations deploy increased from 88 to 89 this year, contributing to an increase of 24% since 2016.

With this ever-growing suite of applications comes an ever-growing number of user accounts, which poses some significant issues: the burden on end users to remember multiple passwords, support costs, and most importantly, the security risks posed by compromised credentials.

What is a password attack?

But what even is a password attack anyway? By ‘password attack’, we mean any method a bad actor might use to gain access to a password-protected account. Here are some of the most common types of password attacks out there, and the best ways to protect yourself against them.

Phishing

What is it?

Phishing is when a hacker tries to trick an individual into revealing personal password logins or installing malicious code on their device.

Typically a classic phishing attack starts with an email that looks like it comes from a trusted source, like your bank, an ecommerce platform, the government or another source you trust.

That message will usually try to “alert” you to a “security issue,” and say that a password reset is required . Since the recipient believes the content of the message is trustworthy, they carry out the instructions, follow the link in the message and change their password.

How this trick works

The hacker sets up a fake website. The website looks official, from the company or institution you trust but, if you look closely there are almost certainly some warning signals. The address in the browser may not be what you'd expect. The design, look and feel of the site may be highly convincing but this is not an official website from the company or institution. The site may look like *yourbank.com* but check the url closely. It's likely to be something more like *urbank.com*.

Smishing, vishing, spear phishing and whaling

Simply changing the platform from email to SMS (where phishing becomes known as "**smishing**") or phone/voice mail (**vishing**), or adding a further layer of personalisation with **Spear phishing**, (where phishing emails "appear" to come from a friend or a colleague), adds nuance and give new life to to the scam.

And **Whaling**, when a scammer hacks a business by taking on the identity of a senior executive within the company adds C-suite level authority to the scheme too - it's important to keep an eye out for all of these to keep company accounts and data protected.

How to prevent phishing attacks:

- Check for the obvious signs of phishing – poor spelling, grammar, punctuation, poor quality logos and if the salutation is unusual (eg 'Valued colleague' rather than your name).
- Phishing attacks often contain threats urging you to act immediately – be suspicious of these, especially when they involve the transfer of funds or the purchasing of gifts/evouchers.
- Check the source of the email – see if the 'From:' line in the email matches exactly who they claim to be. Check back with the person who sent the email to see if they really did send it.
- If in doubt, check with your IT department to see if it is a genuine email.
- Configure your staff email accounts by giving staff the lowest level of server access and user rights to perform their jobs, so as to limit the potential damage of a phishing attack.
- Prevent staff from checking emails or browsing the web using an account with Administrator privileges. These are user accounts which allow you to make changes (install software/hardware, access files, change security settings) that affect others, so a phishing attack on an Administrator account can be much more devastating.
- Use multi-factor authentication on your email accounts so even if hackers know your passwords they will not be able to access the account.

- Check your digital footprint – only include information on your website and social media that people really need to know about. Hackers use publicly available information about your organisation to make their phishing attacks seem more real. Be aware of what information your staff, partners and suppliers are sharing professionally and personally too.

Man-in-the-Middle Attack

A Man In The Middle Attack (MiTM) is where the cybercriminals secretly put themselves in the middle of a legitimate conversation or data transfer between two participants without those participants being aware of them. The attackers then pretend to be both of the participants, which lets them intercept and log all interactions and any confidential data between both parties and also send out malicious information to them without being detected.

A MiTM attack often has two stages. For the initial interception phase, hackers need to access a poorly secured or unsecured Wi-Fi network, such as public or free Wi-Fi hotspots, and they will look for vulnerabilities like weak passwords.

The hackers can use tools to intercept data sent by the victim. They can also position these tools between the victim and the websites they are using to access their login details, banking and/or personal data.

The next stage is decryption: once the hackers have decrypted the user's data, they will be able to read and use the information. Now the hackers can intercept data from both parties as well as transmitting their own malicious information to create more damage in the future. They can also create a lookalike fake site such as the user's bank website, and use the victim's login information to redirect them there.

Once on the fake site, the hackers can deploy tactics such as pretending to be a chat or messaging service from the bank using the information they have already intercepted. They can then begin a conversation on the real bank's site, claiming to be the victim and using their ill-gotten information to get access to the victim's account and money.

Tips to prevent a MiTM attack:

One of the best ways to avoid Man-in-the-Middle attacks is to implement a Virtual Private Network (VPN). Using a secure VPN will secure your traffic and make it more difficult for attackers to intercept it, by ensuring that all the servers you are sending your data to are trusted. A VPN will encrypt your internet connection on public hotspots to protect any private data you communicate while you are using public Wi-Fi.

You can also implement encryption on your router with Wi-Fi Protected Access. If someone outside your organisation can access your modem and router, in theory they could monitor your internet traffic and capture the data coming into and leaving your device by using "sniffer" technology.

Make sure that you secure your website and web app data by enabling HTTPS, so that there is a secure channel for data transmission between a client and the server using encryption. Also ensure that the websites you are visiting are secure – “https” (with a lock sign) in the URL bar of websites.

Always use strong credentials and multi-factor authentication, particularly on your router administration. These are often not changed from their original setup username and password, making it much easier for hackers to gain access to.

Brute Force Attack

A Brute Force Attack is when cybercriminals use automated software to try to “guess” correct password/user names by going through every possible combination until the correct one is found (some can try 6 trillion password/user name combinations per minute).

Hackers use continuous attempts through these brute force attacks to get hold of personal information including usernames, passwords and PINS. This gives them access to online accounts which means they can post as the user to send out phishing emails. They can also redirect website traffic to malicious sites, infect a website with malware or spyware or any number of other nefarious, reputation damaging activities .

There are different types of these attacks. A simple brute force password attack is where a hacker will try to use logic to guess a password, through commonly-used passwords or from basic research of a user’s personal information. A reverse brute force attack is when attackers will take a commonly used password like ‘123456’ or ‘qwerty’ and use it against a list of possible usernames.

Preventing a Brute Force Attack:

- Use a complex username and password. The more complex your password combination (consider using mixed cases, mixed characters, and twelve digits+) the less likely you will be attacked.
- Educate your employees on the importance of strong passwords and network administration. Remove any unused or old accounts with high level permissions.
- Multi-Factor Authentication (MFA) requires one or more pieces of login information on top of the password for an account. If this is enabled, hackers will be unlikely to have access to your mobile phone or thumbprint, so will not be able to access your account.
- Enable remote access management which can help prevent the risk of a brute force attack.

Dictionary Attacks

Dictionary attacks are a type of brute force attack, playing on our reliance on choosing easy to remember and common words or phrases as passwords, including colours, months of the

year, sports teams etc. Attackers put these together as “dictionaries” to run against lists of usernames.

They can take this a step further by including words that are more personal to the user, such as their place of birth or pet’s name. Attackers can combine techniques from simple brute force attacks and dictionary attacks to launch **hybrid brute force attacks**. These are where bots test combinations using common words and random numbers or characters, such as “londonabc” or “ginger123.”

Tips to prevent dictionary attacks:

- Don’t use a word you could find in a dictionary as a password. Much better to use a single sign-on tool or password manager which can generate and remember strong passwords designed to prevent attacks.
- Limit the number of login attempts after a password failure to five or less.
- Change your passwords regularly – every couple of months – and never use the same password for all your accounts.

Credential Stuffing

Credential stuffing is when the hackers know the combination of both username and password - where credentials have already been stolen, often via the dark web or through phishing. If you’ve been hacked in the past, a likely source would have been your old passwords being leaked onto an unscrupulous website.

Hackers try to take advantage of accounts which never changed their passwords after an account hack. They deploy bots to use this information to access more websites as the victim often uses the username and password on a range of different websites, which they never update. One stolen credential can provide access to multiple websites, particularly as over 50% of internet users will re-use the same password over several accounts.

How to protect against credential stuffing

You can avoid becoming a victim of this technique by being vigilant with how you create and use passwords. Use unique, strong and secure passwords for every account or service you use, and make sure to change your passwords regularly. Like with the other kinds of attack, SSO tools or a password manager can help with this.

In addition, be wary of becoming a victim down the line. Monitor your accounts for any recent data leaks to see if your email address has been affected by these - update passwords that may be vulnerable as a result.

Keystroke Loggers

Keystroke logging is the tracking and recording of every keystroke (an interaction with a button on the keyboard) you make on a computer - often without the knowledge of the user, who has downloaded software believing it to be legitimate only for it to install a keylogger without their consent.

Keylogger tools can record everything from your device to collage your personal data and user behaviour, including calls, microphone/camera footage, text input, emails, GPS data, social media messages etc.

While logging keystrokes can be legitimate (e.g. for providing software feedback) it can also be used by cybercriminals to steal your data, if they have put keylogger malware on websites or apps that you use. Victims are unaware that they could be exposing their bank account details, PIN numbers, sensitive data or passwords all of which could be used to commit identity theft or fraud.

Types of keyloggers

Keyloggers can be either software keyloggers - computer programs which install onto a device's hard drive - or hardware keyloggers - physical parts built into your device.

Tips to prevent keyloggers attacks:

- Enable Multi-factor authentication (as above)
- Scan your devices regularly with the latest anti-virus software. Keep your anti-virus protection up to date to keep your devices secure. Look for antivirus software that includes anti-spyware and anti-keylogger protection.
- Inspect your devices regularly to ensure that no keylogger hardware has been installed on your computer if other people have access to it.

The best protection from password attacks? Reducing the need for passwords

As you can see from the list above, there are plenty of ways that bad actors can exploit passwords and threaten both your employees and business. The obvious way to reduce the risk of these attacks is to limit your reliance on passwords using Multi-Factor Authentication, or even better, think about removing passwords entirely.

By requiring additional factors (biometrics, SMS, mobile notification etc.) for users to gain access to their accounts and sensitive corporate resources, attacks like phishing and brute forcing become much less of a threat to your business. When used in conjunction with a modern identity solution too, organisations can set password policies that ensure a level of complexity and set user access policies to limit impact if an account is compromised.

Protect your employees and customers from password attacks with Okta's suite of identity products, including Adaptive MFA, Single Sign-On and Passwordless Authentication.