

How not to fall prey to p@s\$w0rd attacks

PHISHING ATTACK

In a phishing attack, the attacker tries to trick users into providing their passwords by sending emails that look legitimate.

These emails can be anything from fake bills or password reset links from banks to a login failure notification from a fake Amazon or Microsoft website.



Tips



Double-check the sender's email domain

Attackers try their best to mimic legitimate domains, but with a bit of scrutiny, you can easily spot fake email addresses.



Pause before clicking shortened links

Hover your mouse over the link text and check it. Attackers use shortened links to appear authentic.



Report it to your IT team

Attackers try their best to mimic legitimate domains, but with a bit of scrutiny, you can easily spot fake email addresses.



Verify with the concerned person or organization

If you don't recognize the name in the email address, it's most likely fake.



MAN-IN-THE-MIDDLE ATTACK

Attackers try to intercept your communications and impersonate a trusted authority in order to steal your login information.



Don't connect to free, unknown hotspots

Information sent over unsecured public networks that are not password-protected can be accessed by third parties.



Enable encryption on your router

Encrypted information is harder for man-in-the-middle attackers to crack.



Connect over a VPN when accessing your office's network

A VPN adds another layer of protection by encrypting your traffic.

Tips

DICTIONARY ATTACK

A dictionary attack is a type of brute-force attack where the attacker tries to guess the password by going through dictionary words.



Tips



Use long, complex passwords

A strong password should be 8-15 characters long, with a mix of numbers, uppercase letters, and special characters.



Enable multi-factor authentication (MFA)

This adds an extra layer of authentication to the login process. Attackers will be locked out even if they have access to your credentials.



Change your passwords periodically

Changing passwords every 45 to 90 days invalidates stolen credentials.



CREDENTIAL STUFFING

Credential stuffing is another version of a brute-force attack where the attacker obtains a list of passwords and tries them across services. This method relies on the possibility of password reuse.

Tips

If you are an end user



Avoid using email addresses as usernames

Email addresses have greater visibility. By using different usernames, you reduce the chance of being exploited.



Use a password manager

Email addresses have greater visibility. By using different usernames, you reduce the chance of being exploited.

If you are an IT security professional looking to protect your website



Enable MFA and CAPTCHA

MFA and CAPTCHA are effective defenses against bots that are used to perform credential stuffing.



Block access to headless browsers

Headless browsers can bypass CAPTCHA, so they are indicative of suspicious activity.



Monitor your network and blacklist IP addresses

Check for and block IP addresses that try to log in to multiple accounts.

KEYLOGGING SPYWARE

Keylogging spyware, if installed on your system, can record every keyboard stroke and pass on the information to attackers.



Tips

If you are an end user



Use antivirus solutions

Antivirus solutions can scan your downloads for malware and quarantine suspicious applications.



Don't fall prey to phishing attacks

Malware installations can happen via phishing. Check out our post on phishing for more information.

If you are a sysadmin



Monitor outbound traffic in your network

Keystroke logging spyware is usually programmed to contact malicious C&C servers from your network.



Monitor for suspicious software installations

When disguised as legitimate software, malware with keystroke loggers can go undetected by antivirus solutions.

