

Hownotto fall prey to

OQS5M attacks

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.







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.



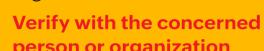
team Attackers try their best to mimic

legitimate domains, but with a bit of scrutiny, you can easily spot fake email addresses.



shortened links

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



person or organization If you don't recognize the name in the email address, it's most

likely fake.

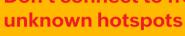


MAN-IN-THE-MIDDLE

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

your login information.





Information sent over unsecured public networks that are not password-protected

DICTIONARY

dictionary words.

can be accessed by third parties.

Connect over a VPN when accessing



harder for man-in-the-middle attackers to crack.



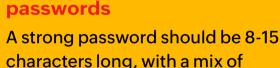
A dictionary attack is a type of brute-force attack where the

attacker tries to guess the password by going through

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



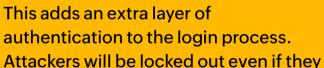




numbers, uppercase letters, and special characters.

Use long, complex

Change your passwords periodically



have access to your credentials.

Enable multi-factor authentication (MFA)

Changing passwords every 45 to 90 days invalidates stolen



credentials.







possibility of password reuse. If you are an IT security

Credential stuffing is another version of a brute-force

tries them across services. This method relies on the

attack where the attacker obtains a list of passwords and

CREDENTIAL

Tips



your website

to perform credential stuffing. **Block access to headless**

suspicious activity.

professional looking to protect

Enable MFA and

CAPTCHA

Monitor your network and blocklist IP addresses

Check for and block IP addresses

CAPTCHA, so they are indicative of

MFA and CAPTCHA are effective

defenses against bots that are used



accounts.

that try to log in to multiple



Use a password manager

Email addresses have greater

visibility. By using different

usernames, you reduce the

chance of being exploited.

KEYLOGGING

Keylogging spyware, if installed on your system, can record

every keyboard stroke and pass on the information to

If you are an end user If you are a sysadmin **Use antivirus**



attackers.



your downloads for malware and quarantine suspicious applications.

solutions

Don't fall prey to phishing attacks Malware installations can





contact malicious C&C servers from your network.

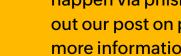
solutions.

usually programmed to

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

Monitor for suspicious





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

Antivirus solutions can scan

