

Office Email Safety Tips

Keeping your computer system safe from viruses and cyberattacks is a full-time job. Email is one of the easier and most common ways phishing scams get into your system.

- **Use a strong, unique password:** Make sure to use a strong, unique password for your email account, and avoid reusing passwords for multiple accounts. Use a combination of upper- and lower-case letters, numbers, and special characters to make your password harder to guess.
- **Don't open suspicious emails:** Be cautious about opening emails from unknown senders, especially if they contain attachments or links. Cybercriminals often use email to spread malware or phishing scams, so it's important to be vigilant.
- **Don't click on links or download attachments from unknown sources:** If you receive an email from an unknown sender with a link or attachment, don't click on it or download it. This could potentially expose your device to malware or other security risks.
- **Be careful what you share in emails:** Think twice before sending sensitive or personal information over email. Consider whether the information you are sharing is necessary and if there are other, more secure ways to share it.
- **Enable two-factor authentication:** Enable two-factor authentication (2FA) on your email account to add an extra layer of security. This will require you to enter a code sent to your phone or another device in addition to your password when logging in.
- **Keep your software and security defenses up to date:** Make sure to keep your operating system and any antivirus or security software up to date to protect against the latest threats.

