

Email Security Checklist for End Users

Following the advice on this checklist will significantly reduce the risk of falling victim to email-based threats.

1. Recognise Phishing Attempts

- ✓ Always check the sender's email address for any inconsistencies or suspicious domains.
- ✓ Be cautious of emails with urgent requests, spelling errors, sender emails address changes domain, or has unfamiliar links.



2. Use Strong, Unique Passwords

- ✓ When creating passwords, ensure the password is more complex by including a combination of letters, numbers, and special characters.
- ✓ Always avoid reusing passwords and ensure each password is unique.



3. Be Cautious with Links and Attachments

- ✓ Before clicking, hover over links to see the actual URL, does it look right?
- ✓ Use antivirus software to scan attachments before opening them.



4. Use Email Filters and Spam Protection

- ✓ Set up email filters to automatically move suspicious emails to the spam folder.
- ✓ Mark unwanted emails as spam to help improve filtering.



5. Protect Personal Information

- ✓ Do not share personal or financial information via email. Personal information can be used to guess passwords or answer security questions.
- ✓ Use encrypted email services that offer end-to-end encryption for sensitive communications.



6. Educate Yourself and Stay Informed

- ✓ Keep informed about the latest email security threats and best practices, cyber threats are constantly changing.
- ✓ Engage in security awareness training and online resources to stay up to date and aware.

