
System message
Ok
MALWARE

Cyber Security Best Practice

Protect your email and online accounts by using a strong and separate password, as cyber criminals can use your email to access many of your personal accounts, leaving you vulnerable to identity theft or a target of fraud.

Install the latest software and app updates, which contain vital security updates to help protect your devices from cyber criminals.

Ensure your home computer system is supported. Microsoft have now ceased support for Windows XP and 7 so pcs running these older, unsupported Operating Systems are susceptible to viruses and malware.

Turn on two-factor authentication on your email and other online applications to make sure your data is secure.

Use a password manager to help you create and remember passwords.

Secure smartphones and tablets with a screen lock offering your devices an important extra layer of security.

Always back up your most important data by backing them up to an external hard drive or a cloud-based secure storage system.

Slow down. Cyber-criminals want you to act first and think later. If the message conveys a sense of urgency or uses high-pressure tactics be very sceptical. You must never let urgency influence your careful review.

Be suspicious of any unsolicited messages or calls. If an email looks like it is has been sent from an organisation you know or trust, do your own independent research. Check the company's website, or a phone directory to find their phone number and call them to verify. Here are some tips on spotting phishing emails:

- Many phishing emails have poor grammar, punctuation and spelling.
- Is the design and overall quality what would you would expect from the organisation the email is supposed to come from?
- Is it addressed to you by name, or does it refer to 'valued

customer' or 'friend'? This can be a sign that the sender does not actually know you.

- Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime.
- Look at the sender's name. Does it sound legitimate, or is it trying to mimic someone you know?
- Your bank, or any other official source, should never ask you to supply personal information from an email.

Do not follow a link within an email or text message. Always be in control of where you are directed online by verifying the organisation.

If a sender appears to be someone you know and trust, if you are not expecting an email from that individual, particularly if the message contains a link or an attachment, always confirm with the sender before opening links or downloading a file.

Never trust an unsolicited download. If you do not know the sender and you are not expecting a file, never open or download it.

Sound too good to be true? If you receive an unsolicited email, or call from a lottery syndicate, inheritance from a distant or unknown relative, or maybe a request to transfer funds for a share of a bounty, it is almost certainly a scam.

Should I pay a ransom to unlock my computer? If your device has become infected with ransomware, the police encourage individuals not to pay the ransom. If you do pay:

- There is no guarantee that you will regain access to your data/ device
- Your computer will still be infected unless you complete extensive clean-up activities
- Attackers may assume that you would be open to paying ransoms in the future
- You will be funding criminal groups


Inbox (9,442)