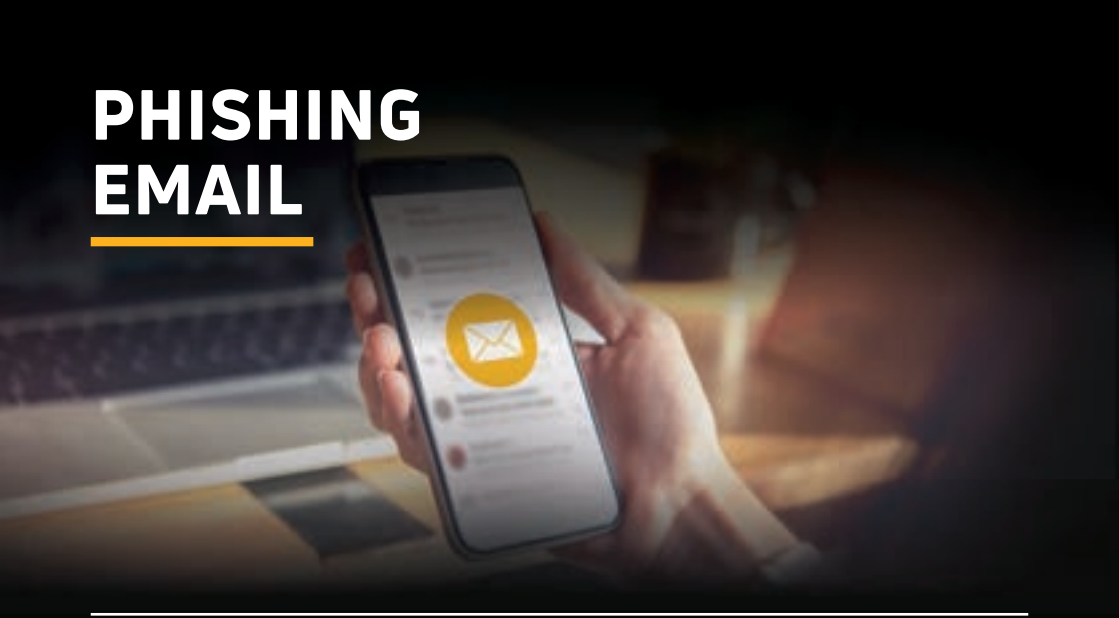
PHISHING EMAIL



Going phishing

Mark the hacker downloads thousands of leaked email addresses from the web.

More than 3 billion phishing emails are sent everyday [1]... one of them goes to Harriet.

Taking the bait

Harriet receives an email from 'PayPal' which she happens to use when making online purchases.

The email offers a discount if Harriet **logs into her 'PayPal' account** within the next 24 hours. The link redirects Harriet to a fraudulent site.

The fraudulent PayPal site **scans Harriet's computer** and downloads keylogger software that can **record every key stroke made.**

Identity theft

With banking and online shopping **passwords known to Mark,** he builds up a profile of **Harriet's online identity.**

The PayPal account shows Harriet's bank details, which are used to pay for a number of **online purchases.**

Harriet's bank account is slowly drained so it isn't noticed.

Mark is also able to see the details of all of **Harriet's friends and family** in her contacts...**they are also targeted.**

HOW TO MANAGE THE RISK

Enable Multi-Factor Authentication (MFA). Preferably do this via authenticator apps or security keys rather than SMS. As a minimum, this should be the norm on all sensitive accounts (banking, primary email, social media).

Always **verify suspicious emails** by checking the actual sender address domain (not just the display name).

If an email asks for action or funds, **confirm the request** using a trusted phone number or a separate communication channel.

Never store passwords in clear text (such as unencrypted notes, documents, or browser auto-saves). Use a reputable password manager to generate and store unique, high-strength passphrases for every account.

Do not rely on poor spelling or generic greetings to spot fake emails. Modern phishing attacks often feature perfect grammar and personalised details.

Don't store passwords where they can be easily seen – draft emails or notes – **consider password managers.**

Be suspicious of email discounts or offers. Always remember that banks will never contact you by email to ask you to enter your password or any other sensitive information by clicking on a link and visiting a website.

If you detect a phishing email **mark the message as spam and delete it.** This ensures that the message cannot reach your inbox in future.

Never respond to a message from an unknown source. Take care not to click any embedded links. Phishing emails are sent to a vast number of randomly generated addresses. Clicking embedded links can provide verification of your active email address. Once this occurs it may facilitate the targeting of further malicious emails. Even "unsubscribe" links can be malicious. Ensure that the email is from a trusted source and you are, in fact, subscribed to the service.

[1] www.techrepublic.com 11/06/19

ecclesiastical