ROMAX

Do’s and don’ts to help protect you against scam or phishing emails and texts.

What is Phishing?

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.

What is Email Scam or Email Fraud?

Email Scam or Email Fraud is the intentional deception made for personal gain or to damage another individual through email or text message. Almost as soon as email or text message becomes widely used, it begins to be used as a means to defraud people.

How can I protect myself against scams or phishing?

There is no way of stopping scams or phishing emails, but here are some basic tips and advice that may help protect you from becoming a victim.

Most companies will NEVER email or text you asking you to log into their website with regards to a payment, or to check account details. If you receive an email asking you to click a link within the email – DO NOT DO THIS. Try going to your web browser, Search for the company who have emailed you, let’s use Paypal in this instance, go to their contact us link, and then either call them using the number given, or email them from the website giving the basic details from the suspicious email.

Or if you know how to, go to (For example again) Paypal’s app or website and log into your account, if there are any account problems, you will have notifications showing here.

But NEVER use any links that are in a suspicious email.

Continue for things to look out for, and do's and don'ts ›››

ROMAX

Things to look out for:

- ! Some phishing emails or texts may be from a company you don’t even use, or you don’t know the sender
- ! It’s an offer that seems too good to be true
- ! Check the spelling of the company name in the email/text, and all round grammar and how the email/text is written – phishing emails are often (but not always) badly written.
- ! The email/text may not use your proper name, but a non-specific greeting such as “Dear customer.”
- ! A sense of urgency; for example the threat that unless you act immediately your account may be closed.
- ! A prominent website link. These can be forged or seem very similar to the proper address, but even a single character’s difference means a different website.
- ! A request for personal information such as username, password or bank details.
- ! You weren't expecting to get an email from the organisation that appears to have sent it.
- ! The entire text of the email/text may be contained within an image rather than the usual text format. The image contains an embedded link to a bogus site

Do’s and don’ts:

- ☒ Do not open emails which you suspect as being scams.
- ☒ Never give personal information such as username, password or bank details
- ☒ Do not forward emails/texts which you suspect as being scams.
- ☒ Do not open attachments from unknown sources.
- ☑ If in doubt, contact the person or organisation as mentioned above the email/text claims to have been sent by ... better safe than sorry.
- ☒ Do not respond to emails/texts from unknown sources.
- ☒ Do not make purchases or charity donations in response to spam email/texts.
- ☒ Do not click on ‘remove/unsubscribe’ or reply to unwanted email.
- ☒ Most spam and junk filters can be set to allow email to be received from trusted sources, and blocked from untrusted sources.
- ☑ When choosing a webmail account such as gmail, Hotmail and Yahoo! Mail, make sure you select one that includes spam filtering and that it remains switched on.
- ☑ If still in doubt, speak to a friend, or a member of Family who may be able to advise you.

Please note: Romax is not a qualified advisor of internet security, this is best practice advise that we follow internally. Romax Marketing and Distribution Ltd cannot be held liable for actions that you make take as a result of reading this content.