An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

NCSC

NATIONAL CYBER SECURITY CENTRE

Quick Guide: Phishing

De

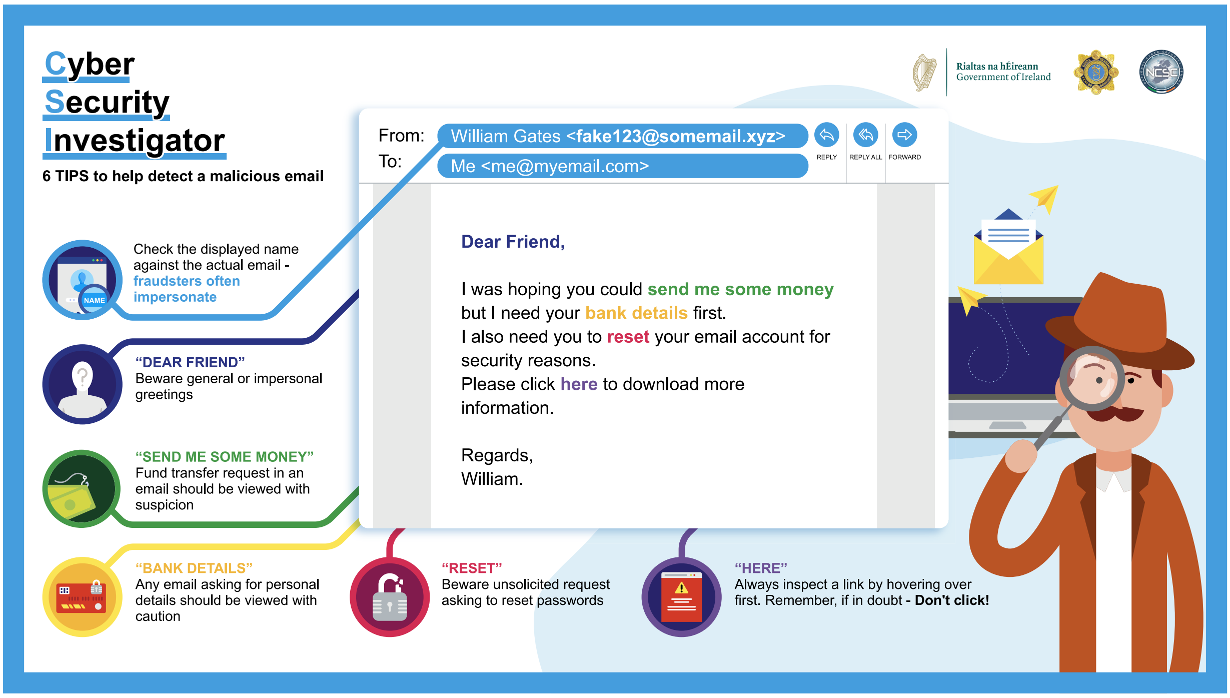
I w
bu
I also need you to **reset** your email account for security reasons.
Please click **here** to download more information.

Regards,
William.

What is Phishing?

Phishing is a type of fraudulent activity carried out by cyber criminals whereby they send disguised e-mails to people or organisations purporting to be from reputable sources to influence the reader to click on links to dodgy websites or to give sensitive information away such as bank details, account passwords or credit card information.

Some phishing emails may contain viruses disguised as harmless attachments, which are activated when opened by the victim. The aim of this type of phishing attack could be something more specific, such as the theft of a business's sensitive data.



Cyber
Security
Investigator

6 TIPS to help detect a malicious email

Check the displayed name against the actual email - fraudsters often impersonate

"DEAR FRIEND"
Beware general or impersonal greetings

"SEND ME SOME MONEY"
Fund transfer request in an email should be viewed with suspicion

"BANK DETAILS"
Any email asking for personal details should be viewed with caution

"RESET"
Beware unsolicited request asking to reset passwords

"HERE"
Always inspect a link by hovering over first. Remember, if in doubt - **Don't click!**

From: William Gates <**fake123@somemail.xyz**>
To: Me <me@myemail.com>

Dear Friend,

I was hoping you could **send me some money** but I need your **bank details** first.
I also need you to **reset** your email account for security reasons.
Please click **here** to download more information.

Regards,
William.

Criminals will use multiple mediums for delivering phishing lures such as:

Email Phishing: Malicious content delivered through email.

Smishing: SMS text messages to a mobile phone.

Vishing: Fraudulent voice phone calls.

Each of these lures will be designed to look genuine, and the sender will usually claim to be a person or organisation that you are familiar with to make it easier for them to gain your trust. It is becoming increasingly difficult to identify these social engineering attempts as attackers become more sophisticated. Attackers take advantage of people's social instincts, such as being helpful and efficient or their emotions such as fear or anger.

This cyber security quick guidance document on phishing has been produced by the NCSC to help you to avoid being phished, spotting the giveaway signs of phishing e-mails, and what to do if you think you've already clicked the attackers bait.

Avoid Being Phished

Criminals will check the internet for peoples publicly available information to make their phishing e-mails more convincing. By thinking about what personal information you and others have about you online there are some easy steps to take to make you a less likely target for a phishing e-mail attack.

All social media platforms provide in depth privacy settings for their users. You can review these settings within your social media accounts and make sure your information isn't publicly viewable.

It's not only you who can post information about yourself online. Be wary of what information your family, friends or work colleagues have posted about you. If necessary, ask them to remove any information about you.

Make a simple checklist you can remember easily by using our giveaway phishing signs (below) to help you to quickly scan e-mails that you aren't too sure about. If you are suspicious of an email that you have received, then report it to your IT administrator or e-mail provider and then delete the suspicious e-mail.

Giveaway Signs of Phishing

As cyber criminals make their phishing e-mails more convincing to try to quickly gain your trust, always pause to consider if an e-mail makes you suspicious. You can still stay one step ahead of them by remembering to scan for one or more of these giveaway phishing signs that could signify you are being targeted by a phishing e-mail.

Does the e-mail begin with a general or impersonal greeting such as 'Dear Friend' or 'valued customer'? If you aren't addressed by your name, then this could signal that the sender does not know you and should not have your e-mail address.

Check the senders email address by hovering your mouse over the 'from' address or clicking the down arrow beside the senders name to reveal more details about the sender. Does the name match the e-mail address and do they look legitimate? If not, the sender could be trying to impersonate somebody.

Is there a sense of urgency to the e-mail such as a request for your bank details or an action to take to avoid losing a service? Your bank or other familiar organisations will never make such requests from you in an e-mail. If you see this type of request, be cautious, contact the organisation directly to confirm.

Always check password reset or authentication requests sent to you by e-mail or SMS. You should only receive these requests if you have requested a password change or attempted to authenticate through your online account. Cyber criminals can send unsolicited requests to steal your passwords, if in doubt, don't click and report it to your account provider.

Are you being offered something for free or at a very well discounted rate? Ask yourself does this sound too good to be true? This tactic is used to panic you into thinking you might miss out on a good opportunity if you don't follow the e-mails instructions. If it sounds too good to be true, it probably is.

Some of these giveaway signs can also be present in text message scams (smishing) and fraudulent telephone voice calls (vishing). The general advice for these types of scams is as follows:

- Shortened and unrecognisable links are a sure giveaway, don't click the bait.
- Honest communications will never ask you to provide personal details.
- If it feels too good to be true or you aren't totally sure of something, then don't engage.
- Contact the organisation directly using their official phone number which should be on their official website to check if they have tried to contact you.

Have You Clicked the Bait?

If you think you've been the victim of a phishing e-mail and have already clicked a link, attachment or provided sensitive information then you can still take these actions to minimise the disruptive effects of the attack.

If you have provided sensitive information such as your password or bank details then change your passwords on all your accounts and contact your bank to get advice on what you should do next.

Use an antivirus software program to run a full scan of your device so it can attempt to uncover any possible viruses and try to remove them.

If you have been victim of a fraud, then you should report this to your local Garda station.

Reporting

Phishing, smishing and vishing scams should be reported to An Garda Síochána at your local Garda station.

Most well-known e-mail service providers will provide a reporting service for various issues. Make sure to check your e-mail provider to see if they provide a 'report phishing' service.

Additional Resources

For more information and resources on phishing please use the following:

NCSC

Guidance: https://www.ncsc.gov.ie/guidance

An Garda Síochána

Cyber Crime: https://www.garda.ie/en/crime/cyber-crime/i-ve-been-caught-out-by-an-online-scam-what-should-i-do-.html

Fraud: https://www.garda.ie/en/crime/fraud

Age Action

Scams and Frauds: https://www.ageaction.ie/sites/default/files/29253-age_action_a5_scams_and_frauds_leaflet_web.pdf

NCSC UK

Spotting phishing scams: https://www.ncsc.gov.uk/collection/phishing-scams/spot-scams

Glossary

Antivirus

Software that is designed to detect, stop and remove viruses and other kinds of malicious software.

Cyber-attack

Malicious attempts to damage, disrupt or gain unauthorised access to computer systems, networks or devices, via cyber means.

Cyber security

The protection of devices, services and networks — and the information on them — from theft or damage.

Multi-factor authentication

The use of two different components to verify a user's claimed identity.

Phishing

Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.

Smishing

Phishing via SMS: mass text messages sent to users asking for sensitive information (eg bank details) or encouraging them to visit a fake website.

Vishing

The fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as bank details and credit card numbers.

Virus

Programs which can self-replicate and are designed to infect legitimate software programs or systems. A form of malware.