GIBRALTAR REGULATORY AUTHORITY

Scams

'Phishing' is a term often used when criminals use scam emails, text messages or phone calls to trick their victims. These are criminal acts usually aimed at encouraging you to hand over money, or your personal or financial information. They may often make you visit a website, which may download a virus onto your computer, or steal bank details or other personal information.

It can be hard to tell if a spam text, email, or call is from a legitimate company or a scammer. For example, scammers could pretend to be from your bank or building society, or they might claim to be from your phone or broadband company.

Scam Calls and Messages

Mobile users worldwide are receiving unexpected calls from different international telephone numbers as part of a massive, global scam with the objective of enticing them to call back. These calls are usually dropped after a few rings resulting in missed calls on the recipients' mobile phones. The recipient is often tempted into calling back the number listed as a missed call. Consumers calling back on these numbers frequently report that they are kept on the line and afterwards discover that they were being charged for higher international rate services. As a consumer you must remember that your telephone service provider does not necessarily have means to determine whether a call is genuine or malicious.

This has on certain occasions prompted the Royal Gibraltar Police to issue public warnings via social media, advising the general public to act cautiously.

How do they work?

The scammers behind these calls mask their real identities. They use automated systems to make high volumes of calls to several telephone numbers within a short time interval. The call often lasts less than a second and comes up as a missed call. If you receive a missed call on your mobile phone from a number you don't recognise, **think twice before calling it back.** That's because there's a chance if you do ring back, you'll fall victim to a scam which could leave you out of pocket. Anyone who does call the number back is charged for as long as they're on the phone.

Most people are left wondering how these scammers got hold of their phone numbers. Although there are different ways and means of sourcing phone numbers, in general these scam calls are often made to sequential phone numbers within different number ranges. By targeting a whole number block, it is highly likely that a percentage of persons utilising numbers from the block will call back.

One may question what benefits these scammers gain from making such calls. The formulas vary, from them receiving cash returns for each call back to more invasive scams which lead the innocent parties to divulge personal and financial information and make them vulnerable to blackmail, fiscal loss and/or identity theft. This is a pressing issue for mobile users and service providers globally are working and collaborating to tackle these scam calls.

What can you do?

The GRA advises that those in receipt of unexpected calls from unidentified international numbers follow these tips to protect their interests:

- Do not answer calls from unidentified international numbers immediately since typically these are dropped after a few rings.
- Genuine callers would usually let the phone ring several times before dropping the call and would also re-attempt to call again if previous calls have not been answered.
- Do not return any missed calls from unfamiliar international numbers.
- If a call is returned unintentionally, you should end the call as soon as possible to minimise the costs incurred. Also, one should under no circumstances disclose personal information over the phone.
- Be wary of false urgency – scammers may try to create a sense of urgency to persuade you to do what they are asking. Be wary anytime somebody tries to persuade you that you must act now.
- Block incoming calls from unknown international numbers using any available phone blocking features.
- Call blocking features will stop future incoming calls from numbers which have already been blocked on the same phone. However, this functionality is not available on all phone models and their capabilities also vary from one model to another.
- Inform your telephony service provider of any unfamiliar international numbers from which calls are being received. Service providers will make use of this information so that they may block outgoing calls to these numbers, thus preventing any harm to clients who return such calls.

- Store international numbers of persons and entities you communicate with in your phone's contact list, this would reduce the chance of mistaking calls from these numbers with unwanted calls.

- To prevent making accidental or inadvertent calls (such as dialling a number when your phone is in your pocket or bag, for example), remove the suspicious number from your call log.

- In line with the advice issued by the Royal Gibraltar Police, consumers should under no circumstances disclose financial, personal, or confidential information over the phone.

- If you believe you have fallen victim to a missed call scam, contact your provider as soon as possible. Depending on the nature of the call, you may wish to advise another entity for example your Bank etc.

Remember!

If you receive a suspicious phone call and are still unsure what to do, simply remember the following three steps:

Stop! Do not give out any personal or bank details.

Hang up and try to carry out some of the checks described above to check if it is a scam call.

Report to your service provider as well as to the Royal Gibraltar Police.

If you receive a suspicious text message or email!

Stop! The text could be a scam. Read carefully and look for any details that do not seem right.

Don't clink on any links or give out any personal or bank details.

Report any suspicious texts or emails to your service provider as well as to the Royal Gibraltar Police and make your friends and family aware too.