Phishing

Don't get caught!

Phishing Basics

Have you ever received a message from…

WhatsApp – saying you have a new voice message – click the link to listen.

Amazon – saying that a parcel has been dispatched from your account, and giving a false name and address.

HMRC – saying you're due a big tax refund.

If something seems unusual, too good to be true or just slightly strange – it probably is!

Also known as '***Vishing***' (via the phone) or '***Smishing***' (via sms), ***Phishing*** is where a fraudulent company disguise themselves as a brand or company which is familiar with you, in order to attempt to receive bank details, passwords or other personal information.

They could contact individuals via phone, text or e-mail and direct them to their fraudulent website via fake pages that look almost **exactly** like the real thing.

Top Tip!

Check that websites are genuine by looking for the **padlock** beside the URL. This means that it is **https** (i.e. a secure site where other users cannot see you personal details). Any website where you are required to **login to** an account should display this.

enquiries@ineqe.com
02890 232 060

How It Works

Phishers will try and get **personal details** in order to **steal your identity,** which can give them access to bank accounts, or simply trick you into sending money. They could do this by asking you to **download an attachment** which (unknowingly to you) contains a **virus,** or by sending you to a website which looks authentic then tricking you into **entering bank details** or **revealing a password**.

Make sure you don't take the bait; reveal your inner detective and suss out a scam by:

Checking for **poor grammar** and **spelling**, while reputable companies scrutinise their e-mails before sending them out – criminals may be hastier, therefore spelling mistakes are often a sign that **something isn't right**.

Hover your mouse over any **links** and a yellow box should appear with a link inside it – this shows the destination of the link. If it doesn't match where the e-mail **said it would go to**, **don't click it**. For users on a phone or tablet, tapping and holding the link will show the URL.

Remember; **real companies** should **never** ask you to reveal passwords via e-mail, so if they're asking you to sign in, or for passwords, or bank details **be suspicious**.

If a company phones you out of the blue and begin to ask for bank details be **cautious**.

Phishing scams will often use **threats** to scare you into action e.g. threatening that your bank account will be **suspended**.

Check the e-mail address it's **sent from**, phishing e-mails often use a recognisable e-mail address, but when you actually click on it, it will be a completely **different address**.

INEQE GROUP

enquiries@ineqe.com
02890 232 060

h2b safer

In The News

Recently, police in Scotland issued a **warning** after telephone scammers were successful after targeting **local pensioners**. The fraudsters pretended to be from business companies, or from banks and encouraged the elderly victims to **transfer their cash** to another account, or to share their **personal details**.

A 74-year-old woman from Dundee lost £140,000 after being scammed by men claiming to be from the fraud department of her bank. Her bank is trying to retrieve the money.

The police advised residents to be "*alert to any phone call they receive from a person claiming to be from a bank, financial institution or business company, either asking for money to be transferred or asking for a phone call to be made to the bank.*" and advised **not to provide any details** over the phone.

What to Do if You Realise it's Fraudulent

- Mark any unwanted emails as **spam** before you delete them.
- If it's a social media page, **report** it.
- Report any phishing emails/calls/websites/texts or social media sites to **Action Fraud**.
- If it's a phishing call report it to the **Telephone Preference Service** (TPS).
- If it's a phishing e-mail **claiming to be from HMRC,** report it to their team phishing@hmrc.gsi.gov.uk.

Action Fraud

0300 123 2040
www.actionfraud.police.uk

TPS

0300 123 2040
www.tpsonline.org.uk

Victim Support

0808 168 9111
www.actionfraud.police.uk

Don't miss out on future information, sign up to our FREE service for Professionals, Parents and Carers at;

www.ineqe.com/professionals

and receive the updates directly to your inbox!

h2b safer a part of INEQE GROUP

Ineqe Group Ltd
3A Heron Wharf
Belfast
BT3 9AE

Telephone: +44 (0) 2890 232 060
E-Mail: enquiries@ineqe.com
Website: www.ineqe.com