Five tips to avoid scams

Contacted out of the blue Legitimate organisations will never contact you 'out of the blue' about important matters. Recent examples have included email or phone messages purporting to come from HMRC (Her Majesty's Revenue and Customs) offering refunds during the current crisis or your bank warning that some security breach has been identified in your account. Such scams aim to get you to provide your bank account details – **don't!**

If the real organisations need to contact you they will usually do it by post but if they do need to use phone or email they won't ask you for personal account details.

Personal details Never give cold callers your personal information. For example, don't give them your personal details to apply for refunds or government benefits on your behalf. As soon as the call/email starts to ask you for personal details, **end the contact.**

A subsidiary part of such scams as far as emails are concerned is to ask you to click on a link (blue) in the email to go to their website to carry out the instruction(s). It is so easy to copy the logos and apparent details of 'official' sites – take a look at the official logos used across our website! What criminals do is copy your bank's website into their own 'data harvesting' site hoping that you will log onto it from the email link and then enter your personal account details, passwords, etc. **Don't be fooled!**

If you want to check what they are saying, log off your emails and then look at a recent bank statement to find the official website's web address (URL to geeks) and log in at that. Look for an email address for enquiries and use that to send a message to them reporting the email contact you've received. They will be keen to know if there are scams aimed that their customers and if their contact was legitimate, they will be able to bring you up-to-date.

Transfer funds Banks will **never** call you to ask you to transfer your money into another bank account if they think your account security is at risk.

Pressurised to respond quickly Scammers will often want to push you to rush a decision and not take the time needed to think it through. Take a moment If something seems odd, take a moment out to think it through. **Don't do anything of a security nature that is pushed as urgent, vital, critical or any other do-it-now word or phrase.**

Contacts from banks and other financial organisations may be to inform you of security issues but these calls won't ask you to provide account details – they are just to inform you of the organisation's response to something unusual. For example, many banks/building societies keep an eye on your account and will inform you if something odd happens such as a purchase well outside your usual geographical area or one that is exceptionally large. Both of these might be legitimate since you have gone on holiday or are buying a new item, but it is useful that your account is being monitored. Whatever the contact you receive, it will not ask you for account details to confirm the communication but will ask you if the purchase was legitimate.

Check the details and ask a friend or relative for their opinion. This is also something to do as a first check. If you telephone shows the callers phone number, check it against your printed account material or similar. If the caller's number is withheld, be suspicious. Hang up and get their official number from your paperwork and then ring them back.

For email, find the email in your inbox and hover your pointer over the sender – a box will pop up with the email address of the sender. Check that it matches the email contacts on your account paperwork. If the email address of the sender is different – maybe only by one letter – from the official one, **delete the email.**

Updated 28th April, 2020