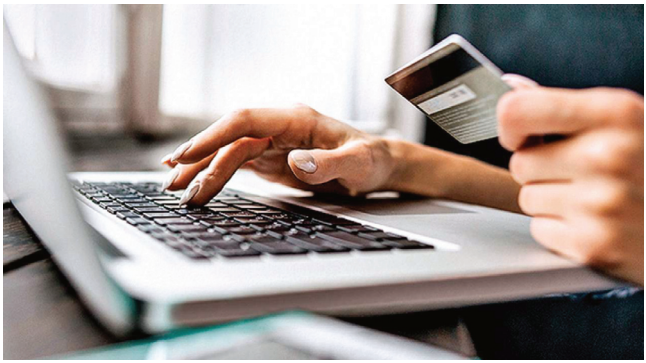
Cyber Security – be vigilant

By Mark Mackin, Mortgage Adviser

It's natural that as we get older things become increasingly complex and challenging. Unfortunately, it has always been that way. As new generations come along, the familiar lies in the past.



This has never been truer than it is today where so much of our lives are played out online, from communications and social media, to banking and shopping. For that reason, it has become even more important to be vigilant to the threat from fraudsters and scammers.

While we can never be 100% secure against all potential risk, constant vigilance and staying up to date with current trends can be key to minimising those threats. That includes having up to date software on phones and computers, because those updates can contain protection to new known threats on the internet.

One of the most common tactics fraudsters use is Phishing scams, which can target huge numbers of individuals all at once.

When receiving an email, use these quick checks to keep your data safe;

- Are you expecting this email? Is its receipt completely out of the blue? Is it from someone or somewhere you haven't heard of before?
- Look at the sender's email. Does it appear to originate from the business or person that it claims?
- Who is it addressed to? Typically, fraudsters will obtain your details through your email account and won't have your full name, so you may notice that the email is addressing you: Dear ABC123@gmail.com
- Some more complex scammers will attempt to cover the account and make it seem like the email is being sent from a legitimate source. This is known as Spoofing. In most cases, if you hover over the sender's email it will show you the actual address.
- Pay close attention to the content of the mail. How does it read? Are there spelling or grammatical errors throughout? Does it contain a mixture of different fonts or text sizes?
- What is the content of the mail asking? It is very rare that banks or businesses will request personal or sensitive information via email. If the sender is requesting the transfer of funds unexpectedly, that is a red flag, but you can always check it out by giving the sender a call. Make sure you are 100% confident that it is legitimate before you open any attachments, click any links or send any information.

But it is not just through email or a text that fraudsters may try to access your details. They often make phone calls and masquerade as a legitimate company such as your bank or credit card provider, HMRC or a local charity.

So take a moment to consider the nature of the call. Is it unexpected?

What kind of information are they asking for? Legitimate companies will never request sensitive information such as your full bank account details, PIN numbers or passwords, over the phone.

The golden rule is if in doubt, hang up and call the official number for the company. You can find that number on paperwork or doing a search on the internet. Don't call a number given to you by the caller.

MONUMENT
MONUMENT FINANCIAL SOLUTIONS

32 Belton Lane, Great Gonerby, NG31 8NB
01636 858551 / 07984 108067
www.monumentfs.co.uk | mark@monumentfs.co.uk