Cyber security – don't ignore the threat

Mark Lofthouse, CEO of Mortgage Brain.

Cyber security is real. And big business. Whether it's people using ransomware to extort money out of the NHS; hackers after information, or spam emails attempting to con individuals out of their life savings, the numbers of criminals wanting to steal your information – and your money - has never been greater.

There were 700,000 attacks per week in 2017, and some big commercial operations – Uber, Yahoo and Equifax – were affected.

For brokers, who handle not just their own information and money, but also a lot of sensitive client documents such as passports, banks statements and payslips, cyber security should be very high on the agenda.

So how can broker's best protect themselves, and their clients, against cyber-attacks?

Let's start with the basics. Any good cyber security system is built on the foundations of an effective anti-virus software and a robust firewall. Clearly there is a balance between stopping potential threats and stopping everything, but the best software will be effective against most malware, spyware and attempts to gain illicit entry to your systems.

The software should be checked regularly for updates (if possible, allow the supplier to install them automatically) and replaced when necessary.

Make sure your operating system is supported. Microsoft, for example, no longer support Windows XP or Vista, so if you still use those they won't be updated and you'll be vulnerable. This has the knock on effect of making your anti-virus and threat scanning software ineffective.

Have passwords that are original and don't use 'Password1'. Consecutive numbers and children's names are also weak, so come up with something that's hard to guess, and intersperse it with numbers, symbols and capital letters.

Use Cloud storage. Cloud storage is run by companies who are professionals in protecting your information from both virtual and physical threats, so can offer a better level of security. Cloud storage also has the advantage of taking information off your computer, so if you do suffer a data breach there's less to steal.

And back up regularly. Losing data is bad enough. If you can't access it by another method, however, your business will suffer yet more damage. Make sure both your main and back-up drives are encrypted.

IT security is a specialist business, so it makes sense to ask a specialist. Companies can advise you on the best protection for your needs, or come and test your existing systems for vulnerabilities.

All the above, however, is only half the battle. The weakest link in any cyber security system is people!

Consider this fact: in 2016, a study from the University of Luxembourg found that 48 per cent of people would reveal their password to a stranger for a chocolate bar.

And that's just the start. Everyone knows someone who has left their smartphone or other mobile device on a train, leaving them (and by extension your business) vulnerable to attack. People open phishing emails and click on dangerous links all the time, effectively giving criminals a free pass to all your files.

That's why a broker's cyber security needs to extend far beyond the technical. Training people to check every email for authentication, no matter how genuine the address might look; to not click on every link, no matter how enticing it may look, is your best defence against being hacked.

Be especially cautious if the sender doesn't address you by name or uses bad grammar, or if the URL is long and complicated.

All the above is particularly true when dealing with private accounts, whose holders probably won't have the same level of security as you.

And while the security in your office may be first class, what about on your team's mobile devices? A system is only as good as its weakest link, so make your sure staff keep their defences up to date on their private systems.

This is particularly true with the increase in 'work from anywhere' capabilities. When working from a public space with shared Wi-Fi, you should be extremely careful what you share online.
Remember that these days we keep information everywhere – Facebook, Twitter, LinkedIn etc. While that may not seem immediately relevant to a broker's business, if for example, anyone can see your Facebook page, and the system password is the name of one of your children, the potential for hacking is obvious. Check all your social media settings to ensure you're not vulnerable.

If your system does gets hacked, and sensitive information or money is stolen, your reputation and liquidity will suffer. If the damage to either is severe enough, you may never recover.

Effective cyber security is now more important than ever. Don't neglect it.

Mark Lofthouse is Chief Executive Officer of Mortgage Brain, a Microsoft Gold Certified Partner. He can be contacted on 01527 557203 or mark.lofthouse@mortgage-brain.co.uk.