Cyber Security top tips – how to be safe in your dealings with LA

AUTHOR / KEY CONTACT

Gerard Chalkly-Maber
Solicitor

Gerard.Chalkly-Maber@LA-Law.com
01202 597798

Law firms and their clients are increasingly becoming targets for cyber criminals and hackers with there seeming to be a headline each week detailing how firms or clients have been attacked in some way.

Whether it be by hackers intercepting e-mails containing firms' bank account details and amending them to their own before sending them on to clients, or hacking into the firm's database to access personal, and often sensitive, information to name a couple of examples, cyber-security is a hot topic.

As an individual, it is of the utmost importance to be vigilant when considering your own cyber security in your dealings with LA. We have come up with the following tips and points to contemplate:

1. ## Have a strong password

   Change your passwords regularly, even perhaps opting for a passphrase instead of a word, e.g. !ae25deWwf (I always eat 25 doughnuts every Wednesday without fail). Such phrases are much harder for hackers to hack when compared to a password which is the name of a pet or your favourite holiday destination. You can also use a password checker to determine your password's strength, e.g. https://howsecureismypassword.net/.

   Also try to avoid using the same password too often because if it becomes compromised, it will not take hackers long to access everything that is protected with that password.

   Using a variety of different passwords is recommended. In an ideal world you should have a different password for each website or service you need to log in to, but this is not always practical. What is recommended is that you consider the security likely to be in place on those websites you use and avoid reusing passwords that could be compromised. For example, if you are a member of a local gym or society then it is probable that their cyber-security is not as robust as your bank, so you shouldn't use the same passwords for both.

2. ## Confirm our bank details before sending us money

   We will have given you either our full bank details or an extract from our bank details in our letter of

engagement. If you receive an email or a telephone call that purports to be from us and which asks for money to be sent to a different account or confirms the email it is probably a scam. Even if the email has attachments that look to be on our letter heading or use our bill forms, do not send money to the new account without first telephoning us and speaking to the person dealing with your matter to check whether it is genuine.

More generally, whenever transferring money, carry out as much verification as you can that the bank details to which you are being asked to transfer money are correct. Emailed details, even in a PDF attachment, can be amended convincingly and you can be easily tricked into sending your money to the wrong account and it will most probably never be seen again.

3. ## Verify unusual correspondence

If you receive any form of correspondence from us and you are unsure about its credibility (e.g. due to tone of language, unusual and unexpected attachments, or something else out of the ordinary) then simply phone us to verify. It only takes an extra 1-2 minutes to make sure.

4. ## Protect your devices

Ensure that any device you use to access the internet is properly protected from unauthorised access. For PCs, laptops, Apple Macs, etc. this involves having a strong login password. For Smartphones, tablets, iPads, etc. then consider using a 6 digit PIN rather than a 4 digit one, or better still, use biometric security, such as fingerprints, if possible. It is also a good idea to lock away any devices that you are not currently using to ensure that they cannot be stolen, nor any of the data stored on them be accessed and removed.

5. ## Exercise cautious browsing

Only use your own computer or device and a trustworthy network to browse websites that deal with and process sensitive information, e.g. online banking. Public or Guest WiFi networks are not always entirely secure and are a prime target for hackers trying to access your device. Being more aware of where and how you access the Internet could help safeguard your online activities.

Also consider installing virus protection software on all of your devices, not just your home computer or laptop. This includes mobile phones, iPads and other smart devices.

There are, of course, many other points of which to be aware in relation to cyber-security and so the summary here is only a starting point. Try to keep up to date with the current threats as the ways in which hackers can seek to access data are always evolving to overcome the protections that are put in place.

Tel: 0344 967 0793 | Email: info@LA-Law.com | www.lesteraldridge.com

Please do not hesitate to contact us should you have any questions regarding any of the above.

Tel: 0344 967 0793 | Email: info@LA-Law.com | www.lesteraldridge.com