Cyber Security Training

Cyber security is defined as the protection of data, networks and systems is a critical issue for Industry and Government. Almost every business relies on the confidentiality, integrity and availability of its data.

This is especially important in a Solicitors office as we deal with confidential information about clients and make multiple financial transactions.

It is important to be aware of different ways we potential could have a breach in cyber security:

1. **Emails** – Emails can be one of the biggest risks of cybercrime. A Hacker if have you email can send you fake emails by changing one letter eg. A1-law.co.uk, Through this they can request bank details and other sensitive information. It is important to check email addresses and confirm details. It is also important not to open any emails that looks like malware, if you download an attachment or open a link the hacker will then have access to your system.
2. **Public Space** – There has been a few incidents when a solicitor was on a train with documents spread on a table doing work, someone has walked passed with a mobile phone on record to purposely collect the details of the pages, these have been leaked out to press, internet and clients details are obtained for identity theft.
3. **Confidentiality** – In a firms there are higher profile cases and clients, something so simple as to "guess who I spoke to today" can spread, if a hacker finds this information they will hack into the law firm and then take the details of this client or case and have in the past held the firm to ransom.
4. **Internet** – It is important to know what sites you are accessing, websites can have pop ups which when clicked by mistake can install viruses and malware.

The Above shows how vigilant as a firm we have to be, although some of the things you might think are silly they have all happened to major firms around the country, cybercrime is growing as technology gets more advanced, it is important to follow steps to keep systems secure.

We are liable if any of the above happens and there are many cases of firms collapsing due to poor judgement. Going forward we need to:

- Check all emails – do not open links or emails if not sure what they are, just delete or speak to Dan / hosted desktop.
- If a website says insecure do not follow the link and close off immediately.
- Do not download anything unless it is from a trusted source.
- Do not work on files in a public domain, this can cause breaches in confidentiality
- Confidentiality on cases and clients is to be adhered to at all time, we need to be as air tight as we can.
- **ALL** bank details need to be confirmed with client over the phone when it has been emailed through.