Ransomware

Ransomware is a form of malware that encrypts the data and files on a computer. The malware is normally downloaded as a result of:

- Receipt of a phishing email with an infected attachment. This attachment is often titled “invoice” or similar that the recipient may usually expect to receive. By clicking on the attachment the malware is installed onto the computer; or
- Clicking on a hijacked hyperlink on a website.

After the files are encrypted, the user can only gain access to them by inputting an “encryption key”. This key is held by the fraudster who emails the victim and demands a payment, often (though not always) in bitcoins.

It should be noted that although the malware may be installed on one computer it can often spread across the network, infecting other machines, including servers.

In order to gain access to their files, the options available to the victim are:

- Restore the most recent back-up taken (which might lead to some loss of work), or
- Pay the ransom (which has no guarantee that the criminal gang will provide the key, and which rewards the criminal gang for their actions).

Precautions Specific to this Type of Attack

The Technology Committee produced a Practice Note in July 2016 to assist solicitors in protecting themselves against a ransomware attack and information on procedures if they do fall victim.

The single most important precaution is the taking of daily backups and regularly ensuring that these backup procedures are working appropriately.

Also ensure that all software, i.e. operating system, internet browser, anti-virus etc., on all computers is up-to-date.