CYBERSAFE LEGAL

Tips for staying cyber safe

Tip 5: Defending against Ransomware.

Ransomware is fast becoming one of the major cyber threats to law firms and all professional organisations.

Ransomware is a type of malicious software (malware) that cyber threat actors activate to gain access and infect computers and then encrypt the files and data on those computers until a ransom is paid. Usually ransom demands are made in bitcoin.

Listed below a few quick tips to help strengthen your defence against ransomware and to make your firm or organisation more cyber resilient.

1. **Create a culture of cybersecurity and educate all people within your organisation:** It is essential that every organisation implements some kind of cyber awareness training. This should be regularly repeated and updated and should be a mandatory requirement for all staff. Given the fact that approximately 80% of cyberattacks are caused by the actions of someone within an organisation itself, this is fundamental to stopping any malware and especially ransomware.

2. **Back up your computer:** In order to minimise the impact of a cyberattack and mitigate loss or damage, it is always best practice to perform regular backups of your information systems. These backups should also be verified. If you suffer a ransomware attack, backup files can be utilised to restore your system quickly (as long as they have not been infected).

3. **Store your backups separately**: It seems obvious, but a backup should be stored on a separate device (not one that is accessible from your network). For example an external hard drive and always disconnect this from your computer as soon as the backup is completed.

4. **Regularly update software and institute a patch management policy:** One of the easiest ways for a cyber threat actors to access a network or information system is through vulnerabilities in software. Ensure your apps and operating systems are always updated with the latest patches and software updates. Where possible, allow automatic updates on your devices so patches and updates are received and installed as soon as they are released.

5. **Be cautious about clicking directly on links in emails, opening attachments or entering websites.** Extra caution must be taken when opening attachments or when opening attachments or clicking links in emails – even if the email is from a known sender. Take extra care when attachments are compressed or zipped files. Also check a website's security to confirm that the confidential information you are sending it will be encrypted before your provide it.

6. **Use antivirus software, firewalls and email filters:** These are one of your strongest defences against ransomware. Reputable anti-virus software is essential (and in our experience you get what you pay for). It will identify unknown and malicious files residing on your computer. Always use firewalls and email filters and keep them all updated in order to reduce the amount of malicious network traffic.

7. **Never provide personal information to an unknown source.** This is basic cybersecurity when answering an email or responding to an unsolicited phone call or message, Reputable institutions do not ask you for your personal information this way. Social engineering cyber threat actors will try hard to get you to inadvertently install malware and ransomware on your computer so always be wary. Verify independently contact from an unknown source and also be careful if called by someone purporting to be from your IT provider.

8. **Use a virtual private network (VPN) when using public WiFi:** if travelling, do not access work information systems by using public WiFi If necessary, utilise VPNs before accessing the WiFi to ensure that the information you are communicating is protected and encrypted.

9. **Don't think paying the ransom will definitely release your encrypted files:** There is much debate about whether ransom should or should not be paid. Many organisations pay it believing their information systems will be decrypted and accessible, only to find a secondary virus has been activated or the cyber criminal has not provided an appropriate decryption key.

There is also some discussion as to whether paying a ransom is a criminal offence to the extent that it aids and abets a criminal act.

We recommend against paying a ransom. If the above steps have been followed, the risk of a ransom attack being effective is significantly reduced.