CYBERSAFE LEGAL

Tip 1: Keeping your mobile devices safe

When mobile devices are used in business environments as well as for personal use, it is especially important to ensure that they are being protected and are being used safely. The same amount of care should be given to these devices as to your wallet or your personal computer. There are a few easy steps everyone can take to enhance their mobile device security and minimise the risk of cyberattacks and cyber threats.

1. **Physical Security**: By far, the most common way for someone to gain access to a mobile device is by stealing it. Always have your mobile devices with you on your person, never leave them unattended and never leave them in parked cars or in stored baggage.

2. **Comprehensive Password Protection**: Always set up a strong passcode, a PIN to activate your device and a fingerprint lock. Make sure that passwords are different for your business and personal accounts and make sure they are more than 8 digits long with a combination of upper and lower case letters, numbers and symbols. Wherever possible use dual factor authentication.

3. **Keep up to date**: Apply any app updates or system updates as soon as possible as they often will include security fixes and patches. Hackers are aware of all updates and target users who fail to update appropriately.

4. **Protect personal information**: Remember your personal information is valuable, it is like money and is something that needs to be protected. Be thoughtful about who gets your personal information and how it is being collected on websites and through apps.

5. **Don't open unknown links:** With the sophistication of firewalls and anti-virus software, hackers are now targeting mobile phone and tablet users with social engineering techniques in an attempt to get you to inadvertently open a link which downloads malicious software onto your device. Always take care when opening any links or attachments.

6. **Check website security:** Always ensure that the websites you are visiting are what they say they are and are secure. Look for the verification lock and click on it to determine the website security. Always check that the website address is https not http as the "s" indicates that the address is used for secure communication over a computer network, and is widely used on the Internet.

7. **Keep a remote back up of your data:** Some stolen or hacked mobile devices have all their data wiped off completely. Always back up your mobile device data and information to your computer and/or you cloud based server.

8. **Be wary of Public Wifi:** Wifi offers hackers and cyber criminals an easy method of accessing your devices. To stay safe, avoid connecting to public or unsecured (non-passworded) wifi. It is never a good idea to conduct financial transactions or access sensitive data whilst you are on a public wifi.

9. **Always Log out of your accounts**: Staying logged in to your aps and accounts on your devices can be convenient , but if someone gains access they can see the information on the app or account and can use that information for financial gain or to impersonate you.

10. **Use encryption for sensitive or confidential data**: If you store or send confidential or personal information using your mobile devices, it is always best to encrypt this data. This can protect data stored and also data in transit. A Virtual Private Network (VPN) can be useful for transmitting sensitive data, particularly if you are in a public wifi spot