LAW INSTITUTE VICTORIA

CYBER SECURITY ESSENTIALS FOR THE INDIVIDUAL

LAW TECH ESSENTIALS

TECHNOLOGY AND THE LAW COMMITTEE JUNE 2017

CONTRIBUTED BY IAN BLOOMFIELD, MANAGING DIRECTOR, IGNITE SYSTEMS

These are mitigation measures intended to provide an individual with a minimum level of cyber security. It includes information about the rationale for each measure and implementation guidance.

1. PASSWORDS

Measure – Employ good password practices and use a password manager.

Rationale – In most cases, the only thing keeping a hacker from accessing your accounts is your password. Simple passwords make the hacker's job easy. Even complex passwords that are 5 or 6 characters can be relatively easily cracked using the latest tools available to a hacker. A password manager provides a practical and convenient way to implement good password practices.

Guidance

- Use only strong passwords; the longer and more complex a password is, the more difficult it is for cybercriminals to crack.
  - Length: five or six characters are not enough. You need a minimum of 16 for any account that stores confidential or personal information, and a minimum of 10 for any other account.
  - Variety: where possible, use a combination of: lowercase and capital letters, numbers and symbols. Each one of those categories increases the password's strength.
  - Words: never use a word that can be found in the dictionary, including compound words or combinations.
  - Personalisation: never use any names, locations or addresses.
  - Recognition: avoid patterns because they make it easier for a cybercriminal to crack a password.
- Use a password manager for storing passwords, and to help with creating good passwords. Get a password manager that is usable across different types of devices – computers, tablets and phones.
- Do not use the same password on multiple accounts.
- Changing your passwords on any regular basis is not a requirement if these guidelines are followed.

Remember, if someone other than you knows one of your passwords, it is no longer secure.

2. TWO-FACTOR AUTHENTICATION

Measure – Use two-factor authentication for access to cloud applications.

Rationale – Cloud based systems do not have the additional layer of security that a computer has when it is connected to a local network and protected by a firewall. The only thing stopping a cyber-criminal getting access to a cloud system is a username and password. Multi-factor authentication adds another layer of security that significantly reduces risk. Two-factor authentication is a form of access control that requires two different types of evidence to verify the user's identity. Typically, what the user knows (password), and a one-time passcode generated by something held by the user (security token or mobile phone app). An everyday example of multi-factor authentication is using a credit card where you swipe the card and also have to enter a PIN.

Guidance

- Use multi-factor authentication for access to all cloud based systems.

3. EMAIL - RECEIVING

Measure – Adopt a well disciplined approach for dealing with incoming emails to ensure you have taken reasonable precautions before opening an email, opening an attachment or clicking on any links in an email.

Rationale – Email is the primary avenue of attack for cybercriminals - the main route for delivering malicious software, either directly via an attachment or by means of a link to a website intended to compromise you in some way. Employing vigilance and good habits with incoming email is the single most important measure you can take to minimise your cyber security risk.

Guidance

- Social engineering is the most common technique employed as part of an email based cyber-attack. Social engineering is the use of words to manipulate a person into taking action intended to defraud them or compromise their security. You should read every email with this in mind. Any wording that involves some sort of appeal to act with a degree of urgency is almost certainly an attempt at social engineering.
- Don't open an email unless you know the sender and were expecting this email. Remember, there is unlikely to be a penalty for being cautious. If you delete an email and it turns out to have been genuine, you will almost certainly receive a follow-up from the sender.
- Even if the sender of an email appears to be an organisation or person you know, keep in mind that it is easy for a scammer to impersonate an email address and appear to come from someone you know or an organisation you deal with.
- Never click on a link in an email, unless you were expecting the email and, even then, make sure the link is consistent with the email content. It takes very little effort to call the sender and confirm the veracity of an email.
- There are many ways a hacker can make an attachment appear to be something it is not. Never open an attachment associated with an unsolicited email, no matter how compelling the subject.
- It is only safe to open an email attachment where:
  - You were expecting to receive it.
  - You have checked with the sender and established the veracity of the email and attachment.

4. EMAIL - SENDING

Measure – Adopt good practices to minimise the risk associated with the emails you send.

Rationale – Email is taken for granted, but it is one of the least secure ways of communicating. Once you send an email, the process involved in getting to the recipient is hidden and out of your control. The delivery process can involve many steps, traversing a number of systems along the way. The security of the email delivery process has not kept pace with the rate of cyber threats, and as a result it is possible for email to be compromised in various ways.

Guidance

- Avoid sending emails where there are more secure options to communicate the information. Using secured instant messaging, such as Skype for Business, is a good option for communicating small amounts of information, particularly internally within an organisation.
- Never include business confidential or personal information in an email unless the email is encrypted, or the information is contained in an attachment that is password protected and encrypted. Business email services such as Office 365 and G Suite offer email encryption as an option, and there are many ways to secure an attachment:
  - Microsoft Office provides the ability to password protect documents.
  - PDF documents can be password protected using Adobe Acrobat.
  - A utility like WinZip files can be used to password protect a file.
- Never send business emails from a personal email account. It is best to keep personal and business email separate, and as a rule a business email account should be more secure.
- Before sending an email, make sure you have confirmed the legitimacy of the email address you are sending to. You wouldn't pick up the phone and start talking to someone without knowing for sure who you were talking to.

5. SECURITY SOFTWARE

Measure – Protect your computer with business grade security software that includes a firewall, anti-virus and anti-spyware, and keep it updated.

Rationale – Having security software in place on a computer is the final defence if all else fails. Effective security software will greatly reduce the risk of a security breach taking place on a computer, by; blocking the malicious email attachment from executing and doing its nasty work, preventing a malicious download from a high risk website from infecting a computer. Business grade security software has additional features and functionality to deal with a business environment.

Guidance

- Have a reputable business grade security software application installed on your computer. You can check for suitable products here: www.av-test.org/en/antivirus/business-windows-client
- Do not use free versions; these might be fine for a home user but they are not suitable for use in a business.

- Make sure the software is setup so that:
  - The signature database is updated at least daily.
  - There is a full scan of all files on the computer at least weekly.

6. SOFTWARE UPDATES

Measure – Keep all computer software up to date with the latest available version.

Rationale – Prioritised and timely installation of software updates greatly reduces the likelihood of a computer being at risk from an unpatched vulnerability. Software vulnerabilities are weaknesses, and software providers regularly release updates or patches to 'fix' these vulnerabilities. Vulnerabilities are continuously being identified and these are then exploited by hackers, so computers that do not have the software update or patch installed are at risk.

Guidance

- For Microsoft Windows computers, use Microsoft Update and make sure it is setup to automatically install updates. If you are using Windows 10, then Microsoft updates should be taken care of.
- Keep all of the software on your computer up to date by ensuring all updates and security patches are installed.

7. REMOVABLE MEDIA

Measure – Adopt good practices with the use of removable media. Some examples of removable media are: USB memory stick, memory cards (SD), portable hard drives, optical discs (Blu-ray discs, DVDs, CDs).

Rationale – Removable media by its very nature makes information portable and allows information to be easily transferred. Using removable media exposes you to several risks: loss of information (this type of media is very easily lost), including a possible data breach, and introduction of malware to your computer.

Guidance

- When you connect removable media to your computer, it should be scanned using up to date security software.
- Avoid using removable media for storing business files unless it is necessary.
- Removable media should only be used to store or transfer confidential or personal information as a last resort. Confidential or personal information should always be password protected and encrypted if stored on removable media.

8. LAPTOP SECURITY

Measure – Protect files stored on a laptop by enabling disk encryption.

Rationale – Being portable devices, laptops present additional risks, such as being lost or stolen when taken outside the office. Encrypting the files stored on a laptop so that they cannot be accessed by anyone unauthorised mitigates these risks.

Guidance

- For both Microsoft based and Apple laptops, enable full disk encryption, preferably at the time a new laptop is first setup for use.
  - For laptops using the Windows operating system, enable BitLocker encryption. BitLocker is a full disk encryption feature included with later versions of Windows.
  - For laptops using the MacOS operating system, enable FileVault full-disk encryption. FileVault 2 is a full disk encryption feature included with later versions of MacOS.

9. CLOUD SERVICES

Measure – Take steps to protect information that is stored using a cloud service e.g. Office 365, G Suite, Dropbox and iCloud.

Rationale – Cloud based systems do not have the additional layer of security that a computer has when it is connected to a local network and protected by a firewall. The only thing stopping a cybercriminal getting access to a cloud system is a username and password. Two-factor authentication adds another layer of security that significantly reduces risk. Two-factor authentication is a form of access control that requires two different types of evidence to verify the user's identity. Typically, what the user knows (password), and a one-time passcode generated by something held by the user (security token or mobile phone app). An everyday example of multi-factor authentication is using a credit card where you swipe the card and also have to enter a PIN.

Guidance

- Two-factor authentication should be used for accessing all cloud services, wherever possible. Two-factor authentication is an available option for many cloud services. Use the "Two Factor Auth List" website to identify whether a cloud service supports two-factor authentication – www.twofactorauth.org

LAW INSTITUTE VICTORIA

- Don't use personal cloud file storage to store company files. A cloud file storage service used for business purposes should be maintained exclusively for business use.
- Don't use consumer versions of cloud services to store company files. The security and functionality provided by business grade services is generally better suited for business use.

10. PUBLIC WI-FI

Measure – Avoid using public Wi-Fi, and employ safe practices if it is necessary to use it.

Rationale – Public Wi-Fi, such as at hotels and café hotspots, can be compromised leaving you vulnerable to malicious attack. Malicious hackers use Wi-Fi sniffers and other methods to intercept the data that goes through the Wi-Fi network, such as emails, usernames and passwords, browsing history credit card details etc.

Guidance

Avoidance is the best defence, so if possible, don't use public Wi-Fi. A good alternative is to use tethering to your mobile phone.

- If using a Microsoft Windows device, turn off public network sharing. Go to the Windows Control Panel, open Network and Sharing Center, select Change Advanced Sharing Settings, and change the profile to Public.
- If possible use a virtual private network (VPN) to connect. This will encrypt and anonymise your traffic.
- The following guidelines should be followed if a VPN connection is not possible.
  - Limit your browsing to websites where the web address starts with "https://", which means the communication to and from the website is encrypted.
  - Don't log in to password-protected websites, particularly ones that contain confidential information – for example, banking and social media sites, or even email.
  - Don't carry out any important business or financial transactions, including credit card transactions.
- Remember to disconnect when you are finished; don't extend your exposure beyond what is necessary.

11. SOCIAL MEDIA

Measure – Follow good practices in the use of social media.

Rationale – Cybercriminals see social media as just another avenue to dupe and scam people, and also a rich source of information. Maintaining cyber security vigilance when using social media is important to minimise your risk.

Guidance

- Social media platforms are a prime target for malware – be especially careful of clicking on links.
- Use the available privacy settings to maximise the security of your social media accounts.
- Fraudulent and false accounts abound on social media, don't trust posts from unverified sources.
- Scams proliferate on social media, so remain vigilant for scams.
- Do not post information that compromises your identity - home address, home phone number, birthdate. Only publish information about yourself that is necessary. Remember that it only takes quite a small amount of personal information to carry out identity theft.
- Pay attention to your social media accounts. An unmonitored account is at risk of being compromised and used to post false or misleading information, or even worse, used to spread scams or malware.

12. GENERAL

- If in doubt about anything to do with cyber security, get an opinion from someone else, preferably a qualified IT specialist.
- Report anything that appears to be a cyber security threat or a possible data breach – report it to management, report it to ACORN, or if you suspect identity theft, contact iDcare.

RESOURCES

Law Council of Australia - Cyber Precedent:
http://lawcouncil.asn.au/lawcouncil/cyber-precedent-home

Stay Smart Online: www.communications.gov.au/what-we-do/internet/stay-smart-online

SCAMwatch: www.scamwatch.gov.au

Australian Cybercrime Online Reporting Network (ACORN):
www.acorn.gov.au

iDcare (non-profit national identity support service):
www.idcare.org

DATE OF ISSUE: 26/06/2018 **CODE:** WEBFORM