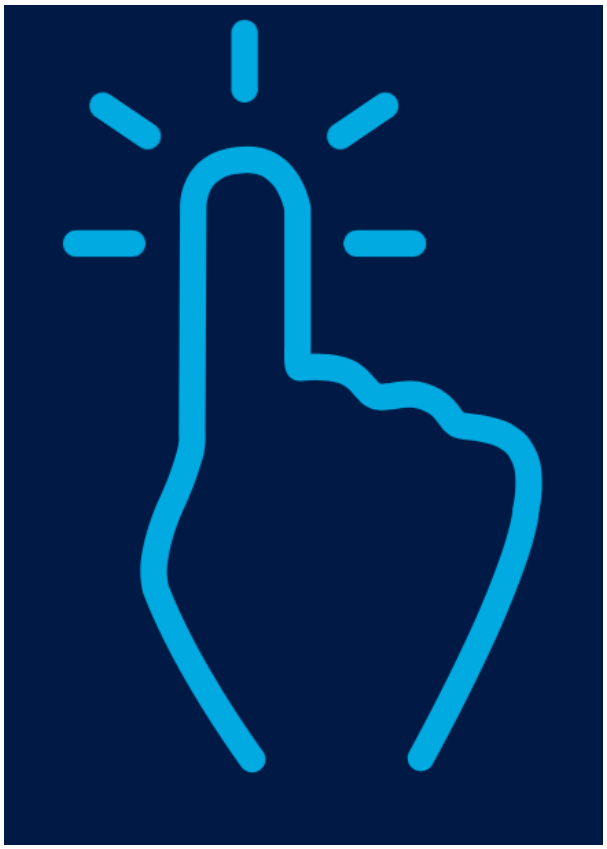
iHelp IT

Cyber Security Book

Helping you with security

4 key online threats to your business



Your security matters to us

iHelp IT is a technical support and consulting company, helping small to medium sized businesses prosper and grow in an increasingly technological world, stripping away the layers of complexity to achieve technical solutions to business problems.

Our engineers focus on support for a large range of products and technologies, and integrate these with business-grade solutions for office networking, email and web hosting, and cloud-hosted telephony.

We understand that the security and availability of our customers data is our highest priority, and provide can advise on how to prevent cybersecurity attachs.

Our top priority with all clients is ensuring their data is secure. We examine existing equipment and cloud services for any hardware, software, or security issues, highlighting any equipment which should be replaced, and ensuring cloud-based disaster recovery services are running.

01. Ransomware

A type of malicious software, designed to block access to your computer until you pay a sum of money. Ransomware encrypts your files without your permission so the hacker can hold your data ‘hostage’ until you agree to pay the ransom.

Like other types of malicious software, ransomware is often circulated via clicking on a link in email messages or via insecure websites.

There are 3 steps you can take to protect your business:

01	Avoid clicking on links or opening attachments in suspicious emails.
02	Use an anti-malware tool to auto-scan all downloads, but note that these tools do not detect all types of ransomware.
03	Backup your important files to a safe off-line location like an external hard drive, so that they can be restored if needed.

Did you know?

Australia Post Ransomware Attack

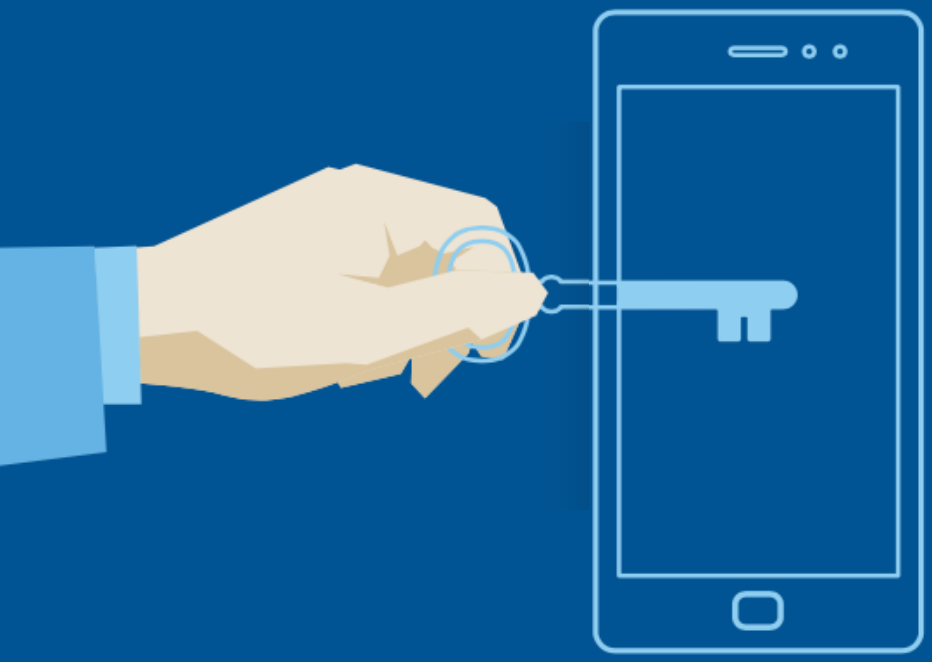
In mid-2014, a number of Australians received an email claiming to be from Australia Post advising a courier had been unable to deliver a parcel to their address.

They were asked to click on a link to view information about the parcel. Once they did, ransomware known as 'Cryptolocker' was installed on their computer.

The ransomware then encrypted all of the files on the computer and demanded payment via a specific website before the files would be decrypted.

02.
Hacking & Phishing

A way cyber criminals try to gain unauthorised access to your desktop computer, tablet or smartphone. Hacking of devices involves compromise of your device's security without your knowledge, often to access or use sensitive, confidential or personal



Deceptive messages

You may be sent a message that claims to come from a reputable organisation you trust or someone you know. The message may ask you to click on a link or open an attachment. This link or attachment downloads a malicious file that compromises the security of your device, providing access to the personal information you have stored on it.

Unsecure websites

Your devices can also be compromised through your day-to-day web browsing activities. The websites you visit may be infected with malware and pass the malware onto your system.

Unpatched software

If you have software installed that is out-of-date, cyber criminals can exploit vulnerabilities that may exist in the software to compromise your device.

Protecting yourself from hacking:

01	Don’t store sensitive information in plain text on your computer or on cloud services such as Evernote, Hotmail or Gmail. Consider encrypted password managers like For Your Eyes Only.
02	Use anti-malware tools to regularly scan your computer for malware. Many can be found for free online.
03	Update and ‘patch’ your software regularly by actioning official updates quickly. Enable ‘auto-update’ options wherever possible.
04	Avoid visiting websites that do not appear reputable.
05	Be extremely cautious before clicking on links or opening attachments you receive in emails, especially when the message is from an unknown source or is out of character (e.g. your bank asking you to confirm you account password). See next page on Phishing tips for more details.
06	If you receive a suspicious email visit the official website of the sender to confirm it is authentic.
07	If you are unsure about the legitimacy of the email message or need help with the above contact iHelp IT for assistance.

Three rules to keep from getting hooked phishing:

Spot the Obvious

- Does the email use emotions to convince you to click on a link or open an attachment?
- Are there some spelling mistakes or grammatical errors?
- Is the text in the email not addressed directly to you, or use impersonal text such as “FirstName”?
- Does the email have a strange “From:” address or a “Reply to:” address that is different to the “From:” address?
- Does the mail have attachments or a link you didn’t ask for, or weren’t expecting?
- Does the link look strange? Hover your cursor over the link without clicking – does the address look unusual?
- Is there an urgent call to action or deadline given?

Remember the basics

- Keep a backup of your data.
- Enable multifactor authentication on every account that offers it.
- Close accounts you don’t use anymore.
- Set up a password manager to keep track of unique, robust passwords.

Listen to your gut

The best way to spot a phishing scheme is to listen to your gut. Examples include:

- Unexpected emails (even from friends)
- Emails with a link to click on
- Emails asking you to check or update information
- Emails which seem rushed or have a strange tone
- A Facebook message when you'd expect a text message

If anything seems even a little bit off, check with the purported sender on **another platform** to confirm that they actually reached out.

- Treat attachments you didn't expect with high suspicion and avoid opening them altogether

If you suspect an email to be a possible phishing attempt you should contact **iHelp IT** immediately. We can quickly identify a email as phishing, and protect you and your employees from the same attack.

03.
Financial fraud

The convenience of online banking and shopping means that cyber criminals can commit fraud on a 24/7 basis from anywhere with an internet connection.

These are the most common financial fraud pitfalls:

Fake websites

Banking and credit card scams often use fake websites that appear to belong to an organisation that you are likely to trust with your financial details. Typically, a message via email or social media that appears to come from the organisation will encourage you to visit the website by clicking on a link. The website will then ask you to provide sensitive information (such as usernames, passwords and account numbers).

Shared computers / Public Wi-Fi networks

When you're out and about, you may need to access the internet via a shared device or a public Wi-Fi network. Poorly secured devices or networks can be used to access your financial information if you undertake activities like banking or shopping in these situations.

Did you know?

Australian banks targeted by SMS phishing scam

In February 2016, the Australian Communications and Media Authority (ACMA) issued an alert warning the public it had received several reports of mobile phone users receiving SMS messages purporting to have been sent by various banks in Australia and New Zealand. The messages advised them they needed to login to their accounts for a number of reasons

(e.g. to verify identity details or view a message sent by the bank).

The SMS messages contained links to websites that, while fake, appeared highly convincing (see below) because:

- They used website URLs that closely resembled those of the banks they purported to come from; and
- The cosmetic design of the fake websites looked professional and closely resembled those of the actual banks

Protecting yourself from fraud

01	Be cautious with unexpected messages from your bank. Never click on unknown links. Manually type the bank's official URL into the browser to verify its liegimtacy.brow
02	Don't use the same password for multiple accounts or online services. All it takes is one account to get hacked and potentially all websites you access with the same password are at risk. Use passwords that are not easy to predict, or use a password generator recommended by your iHelp IT specialist.
03	Be careful when using online banking in public areas where a third party may see your login details.
04	Avoid using shared computers to access online banking or online shopping where you are providing credit card information.
05	Where possible, only undertake sensitive transactions (e.g. online banking or sharing credit card details) using networks you trust - at home or work. If this is not possible use an encrypted connection (look for padlock symbol in your browser) or use a VPN connection.
06	Many banks offer two factor authentication. Use this option where available.
07	Review your daily limit amounts for online banking and consider suspending or restricting telephone banking services.
08	Avoid online banking or shopping using credit cards when in a public Wi-Fi area, such as a cafe. Cyber criminals have been known to pose as customers and generate a fake Wi-Fi network from their device that you then log into, and they can then oversee every keystroke you make.

04.
Payment scams

A range of deceptive schemes where cyber criminals try and obtain money from you under false pretences. Payment scams usually involve attempts to deceive you into providing money or information about yourself that can be used to obtain funds without your knowledge.

Payment scams can be sent to a number of people at the same time, or they may be carefully targeted at certain individuals. These are the most common payment scams:

Unexpected money scams

A scammer contacts you to tell you that you're entitled to a large sum of money in their control. To gain access to it, you need to provide your personal details and, frequently, an initial fee.

Nigerian 419 scams

A scammer gets in touch to offer you a share of a large sum of money to help them transfer money from their own country. They then ask for your bank account details or ask you to provide funds for the transfer fee.

Faked internal authorisations

A scammer sends an email to an employee, using an alias that appears to be from the employee's managing director or supervisor, requesting and authorising an amount of money be transferred to a nominated account. Company websites can be sources of this kind of information.

Dating and romance scams

A scammer gets in touch via an online dating service, developing a relationship over time and often moving contact away from the dating service's website. They then ask for funds to meet unexpected costs or to come and meet you in person.

Charity scams

A scammer pretends to represent a charity or other legitimate cause that is often timed with a well-publicised recent natural disaster or other crisis, and seeks a 'donation' from you.

01	Avoid any arrangement with strangers who are asking for upfront payment from you with the promise of a large reward in return.
02	Be careful of the information you disclose about yourself or your company online, such as role specific email addresses on company websites. This information can be harvested to make the scam more convincing.
03	Many scams have been tried before so search online for the wording in the suspect message to see if if has been identified as a a scam.
04	Research organisations selling products online, and their Google Review ratings and other feedback sources. Ensure they have a reliable and secure payment method before you provide payment details.
05	Where possible, only undertake sensitive transactions (e.g. online banking or sharing credit card details) using networks you trust - at home or work. If this is not possible use an encrypted connection (look for padlock symbol in your browser) or use a VPN connection.

If you receive an email or message (including via social media) that looks suspicious, raise it with your colleagues and contact iHelp IT. You can also forward the email as an attachment to: info@ihelpit.com.au with the subject “Scam Alert”