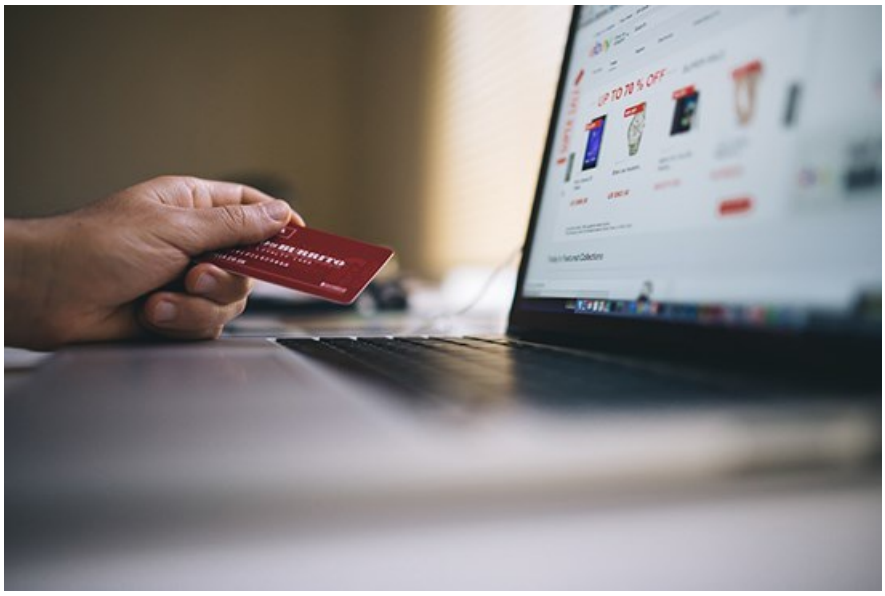
Online vulnerabilities facing small business today

by **BRENDA VAN RENSBURG** *Founder, Australia Learning Code*, and **TIM KENNEDY** *Senior Associate, Kott Gunning Lawyers*

- Cybercrime presents a very real and ever present danger to most businesses.
- Ransomware is one of the fastest climbing online offences in the world today.
- This article covers four online vulnerabilities and offers a guide to help small businesses reduce their risk.



Anyone who uses the internet today, is at risk of cybercrime. According to AimeeO'Driscoll, cybercrime is predicted to cost over $21 billion in damages[1] by 2021 with Australia ranked nineteenth[2] in the world for cyber-attacks.[3] According to Small Business Trends, 43 per cent of small to medium size businesses are targets forcyber-attacks.[4]

Quite apart from the impact cybercrime can have on the internal operations of any business, with the commencement of the *National Data Breaches* scheme, businesses who fall victim to cybercrime, and in particular data breaches, are now required by law to inform both the Information Commissioner and any individuals who may have been put at risk.

This can not only be embarrassing for any small business but can also lead to a loss of confidence which could have severe implications for a business's bottom line.

With the sophistication of most cybercriminals, it can be difficult to stay out of trouble, but there are some

steps businesses can take to minimise that risk. This article will cover four online vulnerabilities and offer a guide to help small businesses reduce their risk.

The password attack

Password vulnerability is one of the most common breaches found in cybercrime. According to *Business Insider*, it takes a hacker less than 0.3 millisecond to crack an easy password.[5] Notably, this makes the 8-character password an easy target for any novice hacker. This becomes even more problematic if this password is also tied to several other accounts, such as bank accounts and online databases, as the ability to hack the password just once can cause security issues for a number of different online aspects of your business.

According to Paul Szoldra, a 12-character password can take up to two centuries to crack, which means that ideally, one should have a minimum of 12 characters in your password.[6] Understandably, the idea of a 12 character password can be off-putting, however, having a password of this length (or longer) does not have to be hard.

Using a combination of words, characters and numbers could make the fear of remembering a thing of the past. A prime example of a combination of this nature is: B1ueEleph@ntpyjamas. Immediately, one can picture a blue elephant in pyjamas. Furthermore, the use of capital letters, the '@' character in lieu of an 'a' and the number 1 in lieu of an 'l', help create a more complex password.

With the sophistication of most cybercriminals, it can be difficult to stay out of trouble, but there are some steps businesses can take to minimise that risk.

Spear phishing

Spear phishing is an email scam aimed at specific individuals within an organisation or business.

The scam email looks like it is from a trustworthy source and leads its victim to a fake website which is often encrypted with malware. According to Kaspersky, cybercriminals use clever social engineering tactics to effectively personalise messages and even websites.[7] Many high-profile executives fall prey to this tactic and thus compromise their computer and network.

A great example of these types of scams are the Australian Tax Office scams where emails impersonating the ATO are sent claiming to have a tax refund due. The email goes on to say that in order to refund these funds to you, you need to click on a link to enter your credit card details. The email looks like an email from the ATO but with some small differences and often the unsuspecting recipient obliges and hands over their credit details.

It is recommended that every email you receive should be treated as a potential threat. However, here are some guidelines to help make your computer and network safe.

- Ensure you scan your emails with anti-malware.
- Look at the return email address. You can be guaranteed that there is something 'phishy' when a sender's address looks something like this: adam@abc.fakeaddress.com.au.
- Stop-Pause-and-Think before clicking on any link or anything inside the email. Most successful attacks

are a result of someone acting in haste. If your instinct is telling you that the email doesn't seem legitimate, it probably isn't.

Trojan horse

The ZBot is a trojan horse that affects Microsoft Windows. The Zbot, also known as the Zeus trojan, steals confidential information, such as usernames and passwords, which are associated with banking and financial information.[8] Although it has been around for a while, the zbot bot is still affecting computers. All it takes is for someone to click on it before it is installed.

The term trojan horse was derived from the well-known ancient Greek story of a deceptive wooden horse that led to the destruction of the city of Troy. A computer trojan horse works in the same manner, often misleading its victim in the assumption that their actions are safe.

The first method of deployment into a system, is through emails. This is one of the more successful methods, as emails can be disguised to look like something important, or even from someone you may know. Notably, one would still need to click on something in the email before it is downloaded into the system. The second method is through clicking on a dubious link in a website. Many times, the user does not even know that the link is malicious.

By adopting the following steps, you can reduce the risk of downloading a trojan on your system:

- Make sure all emails have been scanned by anti-malware.
- Always check the sender's email address. Malicious emails can have small changes in the address either by a number, a letter or even an insertion of a word.
- It is good idea never to click on any link in an email. If you feel it may be important, call the person who sent it. Confirmation is always a good strategy.
- If you visit a website, make sure you double check the link before clicking on it.
- Most trojans can be found on pirated sites. Make it a policy never to visit these sites.
- If you think you may have clicked on something malicious. Run an updated anti-malware scan.

Ransomware

Ransomware is one of the fastest climbing online offences in the world today, with the average ransom demand increasing by over 400 per cent within a space of a year.[9]

The goal of every ransomware is to deny access to the computer, network and/or database. This action is generally linked to an untraceable bitcoin payment. Once this payment has been made, a business is then granted access to their computer, network and/or database. However, once your system has been breached, there is a strong chance that it will be breached again.

Unfortunately, ransomware is a serious risk mostly because the nature of the crime. Even if you pay the ransom amount, there is no guarantee that your database has not been sold. However, one can adopt the following steps to help reduce ransomware attacks:

1. Backup your data on an external (offline) device.
2. Ensure you are running the latest antivirus software.
3. Train your staff about their online activities.
4. Update all your current software.
5. Apply an application whitelist which allows trusted applications to be used on your network.

Conclusion

Cybercrime isn't a fantasy. It is a very real and ever present danger that is facing most businesses today.

Unfortunately, given the speed at which cyber criminals are evolving there is no easy solution to protecting your business. However, taking precautionary steps including getting cyber insurance can help mitigate these risks and ensure a safer online experience not only for you and your staff but your clients as well.

Notes

1 O'Driscoll A, '*100+ Terrifying Cybercrime and Cybersecurity Statistics & Trends [2018 EDITION]*', 25 August 2018 <https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends>

2 Sumo3000, *Top 20 Countries Found to Have the Most Cybercrime*, September 2011 <https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/>

3 Top 20 Countries Found to Have the Most Cybercrime <https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/>

4 Mansfield M, *CYBER SECURITY STATISTICS – Numbers Small Businesses Need to Know*, 03 January 2017 <https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html>

5 Szoldra P, *This website shows how long it would take for a hacker to break your password*, 06 May 2016 <https://www.businessinsider.com.au/hacker-password-cracking-test-2016-5?r=US&IR=T>

6 Szoldra P, *This website shows how long it would take for a hacker to break your password*, 06 May 2016 <https://www.businessinsider.com.au/hacker-password-cracking-test-2016-5?r=US&IR=T>

7 Kaspersky, *What is Spear Phishing*, 02 September 2018 <https://www.kaspersky.com.au/resource-center/definitions/spear-phishing>

8 Symantec, 11 October 2018, Trojan.Zobt , <https://www.symantec.com/security-center/writeup/2010-011016-3514-99>

9 Cert Australia, Ransomware, 2 September 2009.

Kott Gunning has prepared a #cyberthreatregister to help businesses stay informed about data breaches and cyber incidents in 2018.

Brenda van Rensburg can be contacted on australialearningcode@gmail.com.
Tim Kennedy can be contacted on (08) 9321 3755 or tkennedy@kottgunn.com.au.
