# Cyber Security Issues for Small Business

## Introduction

The Australian Government estimates that cyber crime costs the Australian economy more than $15 billion per year and is a cost that many small businesses simply cannot afford.

Small businesses are especially susceptible to attacks from cyber criminals because they are often an attractive target. Unfortunately, due to the size and resources of a small business, they often *“struggle to implement cyber security measures that large businesses routinely deploy”.[[1]](#endnote-1)* (Tam, Rao & Hall, 2021).

Large businesses and government bodies generally have in place IT systems and personnel that can help to manage their cyber security but that is not the same for small businesses.

Everyone is vulnerable to cyber-crime. I received scam messages via sms or email while putting this presentation together.

## What are cyber security issues for Small Business?

Cyber-crime can take many forms, and unfortunately cyber-criminals are developing new ways to attack business all the time.

Common attacks include:

* Hacking – where a cyber-criminal gains unauthorised access of a system or network;
* Malware – where cyber-criminals deploy malicious software to the business’s system. This includes ransomware, viruses, spyware and trojans and the purpose of malware for cyber-criminals is to provide them with a way to access information such as bank or credit card numbers and passwords, or to take control of or spy on a user’s computer. This can lead to fraud, identity theft, disruption, theft of intellectual property or siphoning resources.[[2]](#endnote-2) (Australian Cyber Security Centre, 2021);
* Phishing – where cyber-criminals send fraudulent email messages called lures in order to steal confidential information;
* Scams – where cyber-criminals use sophisticated messages to appear as though the are coming from a business you already deal with, making it difficult to know what is real and what is fake.

There are many many more and businesses need to educate themselves in cyber security.

## Is your business vulnerable?

I want to share a story from an cyber attack that took place on a business I was working at. I was working as a HR and Compliance Manager for a small not-for-profit disability service provider. Part of my role included management of IT assets (though I was at that time in no way skilled or qualified in any IT aspects). There were no dedicated IT personnel and very little structured framework but we used Microsoft 365 for our email handling, document storage on OneDrive, and using the teams and groups functions for internal communication. Around quarter to 5 one afternoon our operations manager came to me and said “I think I’ve been hacked”. I asked for some more information and essentially she had received a message to say that someone in her contacts had received an email that they felt was a scam and when she checked her sent items there was a pile of emails to all her contacts that had originated from her email account. I can’t recall the actual words in the email but there was a pdf file attached and the email basically asked the recipient to open the file.

In a bit of a panic, I immediately suspended her email account, used the system controls with in Microsoft 365’s admin control centre to force a log out of her account from all devices, I manually changed her password and told her to enjoy a quiet night with no email access while I try to figure out what had happened. After a long night for me, researching, checking, learning lots about hackers in a very short amount of time we were able to track the log on to somewhere in the US. A hacker (or possibly a computer program setup by a hacker) had successfully determined her password and was able to access her account. While we were investigating, we found that there had been other unsuccessful attempts to access multiple staff member accounts from all around the world. Fortunately for us, we had been able to respond quite quickly, we established that the email sent from her account was the only thing done by the cyber-criminal and were able to put steps in place quickly to prevent it from happening again, implementing two-factor authentication right away, and forcing regular password changes, but things could have been so much worse!

Cyber-criminals don’t discriminate. They will target anyone, and unfortunately for small businesses, they are an attractive target.

## How can you reduce the risk?

Fortunately, both federal and state governments have dedicated teams working to develop tools and advice for organisations and individuals. The Australian Cyber Security Centre has released a guide specifically for small businesses, called the Small Business Cyber Security Guide.

Some recommendations include:

* Don’t open messages or attachments from unfamiliar senders
* Use SPAM filters if they are provided by your email provider.
* Don’t allow anyone remote access to your computer
* Keep your software up to date
* Use strong and unique passwords and don’t store them in your web browser.
* Enable multi-factor authentication wherever possible.

Other recommendations include:

* Complete a risk assessment of cyber risk for your business
* Implement a management strategy for the risks, which could include things like software design and selection, and engaging an IT professional.
* Investigate Cyber Insurance so that if the worse was to happen, at least you have some financial coverage.

## Summary

Small businesses need to prioritize cyber-security for their business to manage the risk of threats and minimise the financial burden of cyber-crime on their business. There are significant resources available to Australian businesses through the Australian Cyber Security Centre.

## References

1. Tam, T., Roa, A. &. Hall, J., 2021. The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. *Computers & Security,* 109, p. 102385. [↑](#endnote-ref-1)
2. Australian Cyber Security Centre, 2021. *Small Business Cyber Security Guide.* [Online]   
   Available at: https://www.cyber.gov.au/sites/default/files/2021-11/ACSC\_Small\_Business\_Cyber\_Security\_Guide\_V6.pdf  
   [Accessed 28 April 2022].

   Bibliography

   Australian Cyber Security Centre, 2020. *COVID-19: Protecting your small business.* [Online]   
   Available at: https://www.cyber.gov.au/sites/default/files/2020-04/COVID-19%20%E2%80%93%20Protecting%20Your%20Small%20Business%20%28April%202020%29\_1.pdf  
   [Accessed 28 April 2022].

   Australian Cyber Security Centre, 2021. *Small Business Cyber Security Guide.* [Online]   
   Available at: https://www.cyber.gov.au/sites/default/files/2021-11/ACSC\_Small\_Business\_Cyber\_Security\_Guide\_V6.pdf  
   [Accessed 28 April 2022].

   Business Queensland, 2020. *Cyber security for your business.* [Online]   
   Available at: https://www.business.qld.gov.au/running-business/protecting-business/risk-management/cybersecurity  
   [Accessed 28 April 2022].

   Tam, T. R. A. &. H. J., 2021. The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. *Computers & Security,* 109(10), p. 102385. [↑](#endnote-ref-2)