Cyber Security Threats:
How to Protect Your Small Business

Council for Small Business Australia

Our Objective

- This presentation from COSBOA aims to inform you about ways to protect your small business from cyber attacks.

- By the end of this presentation you will:
  - *understand different methods to protect your small business from cyber attacks*
  - *be ready to take the COSBOA Cyber Security Awareness test*

How Can I Protect My Small Business?

There are **four key methods** to help protect your small business.

1. Education. Ensuring that the small business owner and staff are away of cyber security threats, how attacks occur, where vulnerabilities are, and what actions to take to prevent an attack.

2. Software. Purchasing and installing anti-virus and or other software that is designed to protect computers, phones, servers, laptops and other devices.

3. Actions. Ensuring that all staff are aware of actions that need to be taken to protect the business. This includes developing processes specific to your business that are designed to ensure staff are responsive to threats.

4. Insurance. When cyber attacks occur, it could be useful to have insurance to protect your business from costs associated with data breaches, lost days of work, etc.

Education

- It is essential that all small business owners and staff understand how to spot and avoid potential cyber attacks.
- Education is the foundation of our strategy.
- There is a range of resources on the COSBOA website that will also support you in education your team on cyber security.
- COSBOA have also developed an online test for our members to assess the knowledge of their staff. This is a short test which can be taken online and a certificate will be emailed if you pass by 75% or higher. See our website for more information.

Software

- COSBOA recognises that while education is important, small businesses also need effective protection against attack.
- Anti-virus and cyber security protection software is essential for any modern business.
- We have partnered with Symantec to provide a discounted Norton Security package for members.
- This package will help to ensure that your small business is protected if targeted by criminals.
- Head to our website for more information on this.

Actions

It is important to develop processes specific to your small business and ensure that staff follow these procedures to protect the business.

1. Install all software updates automatically
2. Regularly run anti-virus software scans
3. Keep cyber security software firewalls turned on
4. Remove spyware / adware
5. Prevent identity theft through being aware of scam emails and not providing sensitive information via email
6. Avoid opening suspicious emails
7. Never transfer funds until you have checked via phone/ in person with the staff member requesting the transfer
8. Protect your passwords
9. Maintain a regular backup of important files

Install All Software Updates Automatically

- Updates from your software will often contain new information that will fix problems. These are called patches.
- This is particularly important for operating systems, but is also important for programs.
- This is now equally important for your phone, iPad, laptop, computer, server, etc. Make sure that all devices are kept up-to-date automatically.
- You can select the automatic update option via your settings.
- Ensure that you restart the device after installation of updates.

Regularly Run Anti-Virus Software Scans

To avoid cyber security attacks that can be caused by viruses it is important that small businesses install anti-virus software. Anti-virus software helps by removing viruses. It can quarantines and repairs infected files to make your device more safe. Sometimes the software can also help prevent future viruses.

Installing this software is not enough. You must also make sure to regularly run the anti-virus scan associated with the software.

While new viruses are constantly being developed, you can help to protect your small business by keeping the anti-virus software updated before the scan takes place.

Turn Cyber Security Firewalls On

Computer operating systems often have firewalls, but additional software may help too.

Firewalls are designed to protect your device from cyber attacks.

Check to make sure you have a firewall within your system and that it is active.

Firewall scanners can also help to detect where attackers may enter your system. Firewalls can then work to protect the system where possible.

Remove Spyware / Adware

Spyware: software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.

Adware: software that automatically displays or downloads advertising material such as banners or pop-ups when a user is online.

Software like Norton can help to detect and remove spyware and adware from your device.

This is important to keep your systems safe.

Prevent Identity Theft

The following advice comes from the **Australian Federal Police**. To protect identity theft:

- ensure that the virus and security software on your computers and mobile devices is up-to-date and current
- don't use public computers (for instance, at an internet café), or unsecured wireless 'hotspots', to do your internet banking or payments
- only use trusted online payment websites for items won at online auctions or purchased online (e.g. PayPal)
- regularly review your bank statements and obtain copies of credit history reports
- don’t respond to scam emails or letters promising huge rewards if bank account details are supplied, or in return for the payment of 'release fees' or 'legal fees‘
- in relation to social networking sites, always use the most secure settings
- For additional information, see: https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/Protectingyouridentity.aspx

Avoid Suspicious Emails

It is important to be sceptical of unusual emails. Suspicious emails are common and many end up in junk email; however, criminals are becoming smarter. They often use information about you and fake logos, email addresses, etc. to make an email look more authentic.

- Always delete emails — especially those with attachments — from people you don't know.
- Never click on attachments that seem suspicious, even if you do know the sender.
- When receiving an email from a bank or business, check the email address to ensure it is from the authentic sender by checking against the real URL.
- Rather than clicking on embedded links, copy and paste them into Google search which can check where you are heading.

Manage Fund Transfer Carefully

- Over the past few years a new cyber security risk has emerged involving spoof emails.
- The emails look like they have come from your boss/ a client and will ask you to transfer funds to a criminal's bank account.
- Sometimes an email exchange can begin with a simple request and end up with a finance transfer request.
- Always check via the phone or in person to make sure transfers that have been requested are legitimate and that the financial institution details are correct.

Protect Passwords

The following 6 tips will help you to manage your passwords:

1. Pick a strong password – Use numbers, lower and upper-case, and a symbol e.g. Bi78#$no
2. Don’t share your password with others
3. Use multifactor authentication – Where possible, some applications offer multiple authentication steps e.g. text message & password
4. Biometrics (fingerprint) is a good option
5. Use different passwords for different accounts
6. Consider using a password manager like this FREE one from Norton https://identitysafe.norton.com/

Regularly Back Up Files

To lower the risk of losing important files to ransomware, virus, blackout, fire, or other cyber attack/ disaster, it is important to regularly back up all files for your small business.

There are many methods to back up files and COSBOA recommends that you research or consult a professional to work out what is best for your small business. This process should be checked and tested regularly.

One method is to back up your files to a external hard drive that is taken home from the premises at the end of the day. You must store the back up files in a safe place that is external where possible.

Some cloud based storage may be suitable for your business, depending on the file type.

Insurance

- A well-trained staff that understands cyber security combined with quality anti-virus and cyber protection software will work, most of the time.
- Sometimes, there is a new technology or a weakness found in a system that allows criminals into your system.
- When criminals ‘break in’, you may lose valuable data.
- Just like when a building is insured against weather etc. you should consider insuring your business against cyber attacks.
- For interested members, COSBOA has partnered with Epsilon to provide
  an insurance package for our members. See our website for more information.

In Summary

- It is important for all staff to be educated on cyber security and how to manage associated risks.
- Software like **Norton Security** will help protect devices and systems.
- All small businesses should develop strategies and processes to ensure risks are mitigated.
- Cyber insurance like the COSBOA package from **Epsilon** cover businesses in the event of a cyber attack.