Cyber security 101 for businesses

Hack attacks, ransomware and phishing are just some of the cybercrimes against small businesses that can expose them to data theft, extortion or even business failure. There are many steps businesses can take to reduce these risks and potential damage in the event of an attack.

There are many steps businesses can take to reduce these risks and potential damage in the event of an attack.

There are lots of different ways criminals attack businesses online. The Australian Cyber Security Centre (ACSC) has categorised the three main cyber threats small businesses face as malware, phishing scams, and ransomware.

"Cyberspace has become a battleground."

(ACSC annual report July 2021 - June 2022)

Top tips to stay safe online

Prevention is always the best form of protection. Here are some quick wins to help keep yourself and your business safe.

- Turn on automatic software updates – this helps to patch up vulnerabilities and the automatic updates mean you don't have to think about them.
- Cyber training – teach your team how to identify common cyber scams such as phishing emails.
- Use anti-virus software – this helps protect your data from malware.
- Secure your devices – Use locks or encryption, and regularly back up your files.
- Avoid public wifi – use a secure connection, as information can be easily intercepted on public wifi.
- Regularly back up devices – recovering data can be expensive, so make sure you have your up-to-date documents backed up.
- Switch on multi-factor authentication – provide two or more proofs of identity for better security.
- Use passphrases rather than passwords – these are easier to remember and harder to crack.
- Create a Cyber Incident Response Plan – don't wait until it's too late to create a contingency plan for your business.

Should your business consider cyber insurance?

Today, every business is supported by a digital backbone. Which means all Australian firms are at risk of criminal cyberattacks. Cyber insurance offers businesses a level of protection to mitigate the effects of a cyber breach or attack. So, while prevention and practicing cyber safety is crucial, it also pays to take out insurance, so your business can better restore its operations if it falls victim to an attack.

Cyber cover in action: case study

An accountant was the subject of a ransomware attack, in this hypothetical example. The criminals encrypted the network data, locking the business out of its system and disrupting normal operations. Sensitive client data was compromised in the process.

The accounting firm had taken out cyber insurance, so it was covered for the cost to forensically investigate the breach, the legal costs associated with prosecuting the criminals, as well as paying for the funds to settle customers' claims. The insurance policy also met the costs associated with notifying government bodies and regulators of the breach.

While prevention is better than cure when it comes to cybercrime, having insurance cover in place meant the business was able to appropriately defend the attack and recover from it.

Your broker can help

Don't risk waking up one morning to find cyber criminals have locked your business's IT systems. Talk to your broker today about how we can help mitigate the risk of cyberattacks stopping your business in its tracks.

Contact us today

Archer Insurance Corp

Maria Tepelidis

03 8560 1555

maria@archerinsurance.com.au

www.archerinsurance.com.au

ABN: 78 339 722 583 | **AFSL:** 485736

Archer Insurance Corp Pty Ltd