Cybersecurity scams are an issue for all businesses. What can you learn from these epic fails?

Josh Jennings

“Organisations are today faced with a relentless and constantly evolving landscape of attacks and threats that will continue to grow in sophistication and impact.” Those, the sage words of Steve Moros, Cybersecurity Director Cisco ANZ affirm the notion that businesses of all shapes and sizes are susceptible to cybercrime. What really matters, however, is how your business bounces back from a cyber attack and ultimately grows.

In 2018, there were some high-profile cybercrime casualties. In calling attention to some of them here, we uncover learnings that you can adopt to help better protect your own business.

Facebook

2018 might just be candidate for Facebook's annus horribilis. If the Cambridge Analytica disaster wasn't toxic enough, in September the company subsequently conceded that 30 million accounts were hit in another data breach. Hackers accessed personal information including names, relationship statuses, religions, birthdates, workplaces, search activities and location check-ins for almost half of these accounts.

Data breaches, this incident magnifies, can be disastrous for brand reputation and customer relationships. Hackers are all too happy to hold it hostage, mine it for their own intellectual capital and trade it.

A good first step in protecting your own data is to understand its value and ensure your employees do too. It's paramount small businesses protect their data like any other valuable property. You need to lock it down, vault it from anybody who isn't vetted and keep it under surveillance. With the Notifiable Data Breaches scheme now enacted, it's also worth having a Data Breach Response Plan in place for your business.

FIFA

This October, FIFA acknowledged its computer systems were hacked and said it was bracing for the fallout. This is unsurprising since more than 70 million documents and 3.4 terabytes of data have been leaked to German magazine *Der Spiegel*, who has since launched a weekly series detailing FIFA's secrets, warty and all.

It's believed that a phishing scam is the likely cause of the hack, according to cybersecurity experts. Phishing attacks essentially involve cybercriminals sending fraudulent messages by email, SMS,

instant messaging and social media channels in the hope that recipients believe they are from legitimate sources. Often a phishing scam will encourage individuals including employees to click on a link to a bogus website where they're promoted to enter confidential business details such as passwords or credit card information. Some phishing attacks are laughably transparent but others are more sophisticated – and they are becoming increasingly so.

Cybersecurity experts point out that a layered cybersecurity approach is important to protecting your business against phishing attacks since cybercriminals are continually trying to attack from new angles. Cloud-based security platforms such as Cisco's Umbrella is an example of cybersecurity technology that offers unprecedented protection against phishing, malware and other nasties – **you can road test it for free over a 14-day period** to see how it benefits your business's cybersecurity too.

The FIFA hack also highlights why it's important for businesses to use protections such as spam filters, stay alert to the latest threats, educate employees to recognise phishing scams and have a response plan in place in the event a phishing scam does land.

Oops! We could not locate your form.

Tesla

Electric car company Tesla's image took a hit this year when it revealed an ex-employee had hacked its confidential information and syphoned it to third parties.

In a lawsuit the company filed on June 19, details emerged stating that the employee had created hacking software that was living on three computer systems of other Tesla individuals. The software

was enabling the periodic export of data off Tesla's network and into the possession of third parties.

Malicious insider attacks, which can involve individuals committing computer sabotage, extortion, fraud or confidential information theft, are costly. Although they are a real threat to Australian SMBs, many are preventable.

Some of the key steps you can take to protect your business include the following:

- Considering how much you should control information staff access to do their jobs.
- Deactivating employees' system and network access when they finish with the company.
- Promoting a workplace culture of transparency, honesty and fairness to diffuse retaliatory action.
- Educating staff about protecting their own privacy and conducting pre-employment background checks on employees.

Cybercrime adversely affects organisations of all sizes but it's important to recognise these scenarios as opportunities to learn how to better protect your own business from cybercrime.

Learn how to better protect your small business from the impact of a cyberattack. Sign up for a free trial of Cisco Umbrella.