5 tips to ensure your business is (cyber)secure before the festive season hits

By Graeme Millar

8 Nov 2022

With the festive season just around the corner, now is the time of year to pay even closer attention to cybersecurity. From cloud-based data storage to mobile interactions, we rely on an increasing amount of technology in our daily lives. Unfortunately, this means that a potential attacker has more opportunities than ever before to find an opening.

Image source: Saksham Choudhary from Pexels

Many small businesses believe that because of their size, they don't have anything worth stealing. The truth is that there is already a lot of value for any would-be attacker between login credentials that could be used to gain access to other accounts, personal information about your customers or employees, and your payroll (without even getting into the specifics of your industry).

You don't want to be one of the 60% of small businesses that fail within six months of a cyberattack. That is why it is critical to take cybersecurity seriously as we enter the last two months of the year.

Follow these cybersecurity steps to lessen cyber threats to your business:

1. Follow password industry best practices

Did you know that 80% of data breaches caused by hacking involve compromised or weak credentials? Furthermore, regardless of the type of attack used, stolen credentials are used in 29% of all breaches.

Even if you believe your company adheres to best practices for password strength and frequency of updates, a chain is only as strong as its weakest link. You could be in for a nasty surprise if you don't take steps to ensure your team follows suit and understands what's at stake.

Making sure your users understand and follow industry best practices for passwords is the first step for any small business concerned about cybersecurity. That means a unique password for each website and application, as well as long, random combinations of letters, numbers, symbols, and multi-word passwords.

Remembering all of your passwords and sharing accounts with everyone on your team who needs to use them can be difficult. A password manager is essential in a small business where people are already wearing multiple hats. The last thing you need is a sticky note in a desk drawer or on a computer monitor to keep track of everything.

New report reveals the leading brands that hackers imitate the most
26 Oct 2022

2. Establish a patching and update schedule

Unpatched devices are another common source of vulnerabilities for both large and small businesses. As the internet of things (IoT) becomes more prevalent in our daily lives, an increasing number of devices, from printers to watches, are being linked to our business networks. That means more potential entry points for an attacker, especially if a zero-day exploit emerges but goes unpatched.

The solution is to commit to regular patching and updating so that you know every device connected to your network is up to date. It can be a significant addition to your IT staff's workload, so managing IT services (where you can delegate updates and day-to-day network administration to a third party) can free up resources for tackling bigger issues, such as how to integrate technology more effectively into your business.

3. Enhance your cybersecurity education

Regarding cybersecurity, the adage "what you don't know can't hurt you" couldn't be more false. With the growing popularity of spearphishing and other attacks that rely on fooling the humans behind the technology we rely on, it's never been more important to ensure that everyone can identify a suspicious email when they see one.

Creating a security system that is completely resistant to human engineering techniques may be near impossible, but teaching people what to look for and what to do about it can greatly reduce your chances of being caught out. When the average data breach can cost a small business several thousand, it's worthwhile to invest in training your employees to be part of the solution rather than part of the problem.

Inside the mind of the attacker: How cybercriminals think when they enter organisations
25 Oct 2022

4. Employ a reputable IT services provider

Keeping your network up-to-date, secure, and operationally sound is a difficult task for any small business' IT department. You can hire a team of network security experts from a managed IT service provider, giving you the resources you need to fight back without breaking the bank. You get assistance with everything from network connectivity to device updates, as well as 24/7 network monitoring and threat detection, giving you the ability to respond to whatever comes your way.

Working with a managed IT services provider also frees up your internal IT resources to focus on what they do best: assisting you in using technology to gain a competitive advantage. Your IT team can shift from a reactive mindset to a more proactive mindset, looking for opportunities to transform your core business processes and score some big wins.

5. Take action right now

With more and more attacks on small businesses, cybersecurity has risen to prominence in 2022. A single data breach can put your company out of commission, so it's critical to take precautions now to avoid this. It's crucial to remember that cybersecurity does not happen in isolation - to succeed, your entire team must understand what is at stake and what they can do about it.

Conclusion

While cybersecurity is important all year round, it’s even more so during the silly season. To keep your business safe from cyberattacks, use industry best practices for passwords to avoid becoming a target. Make a commitment to a device patching and upgrading schedule, seek assistance, enhance your cybersecurity training to ensure that your team is up to date, and consider hiring a managed IT services provider.

ABOUT THE AUTHOR

Graeme Mllar, managing director of SevenC Computing