TIPSHEET

Protecting yourself and your Data Online

In today's ever-evolving work landscape marked by rapid technological advancements, the need to prioritise cybersecurity at home and at work cannot be overstated. As a business leader or employee, it is crucial to recognise the significance of protecting your sensitive data in the face of increasingly sophisticated and widespread cyber threats.

It's not just about data, though. A successful cyber-attack can have serious consequences for our mental health and overall sense of safety. As these types of attack become more common, it's important to practice strategies to protect your personal wellbeing as well as your personal information.

CYBERSECURITY 101

Cyber-attacks can have devastating consequences for businesses, both financially and reputationally. Rapid advancements in technology might help make our work easier, but it's also resulted in more sophisticated and dangerous cyber practices.

Cybercriminals are quick to adapt and exploit vulnerabilities in new systems and software. They leverage cutting-edge techniques, such as artificial intelligence and machine learning, to develop advanced attack methods and evade traditional security measures.

Added to that, the increase in interconnected devices and the rise of the Internet of Things

(IoT) have expanded the attack surface for cybercriminals. With an ever-growing number of devices connected to the internet, from smartphones and laptops to smart home appliances and industrial control systems, each presents a potential entry point for a cyber-attack. This interconnectedness creates a complex web of vulnerabilities that can be exploited by attackers to gain unauthorised access, disrupt services, or steal sensitive information.

We only have to look at recent cyber-attacks to see why they're so damaging. The Optus data breach was one of the largest breaches in Australian history, as it affected millions of customers. According to the Office of the Australian Information, large-scale data breaches impacted millions of Australians' personal information in the second half of 2022, as part of a 26% increase.

WHAT DOES A CYBER-ATTACK LOOK LIKE?

There are multiple types of cybersecurity risks. Here are some which affect companies and their employees.

Social engineering attacks: Social engineering attacks are used to trick victims into revealing personal information through phishing scams or other 'impersonations' to make the scam look legitimate.

Ransomware attacks: Ransomware attacks, as the name implies, refer to a type of cyber-attack where hackers gain unauthorised access to an individual's or organisation's data and subsequently encrypt it, effectively holding it hostage. In these attacks, the attacker infiltrates a device or network and restricts access to the files, demanding a ransom payment in exchange for restoring access to the encrypted data.

FIND OUT MORE

1300 687 327 info@convergeintl.com.au convergeinternational.com.au

Converge INTERNATIONAL

Man-in-the-middle attacks (MiTM): A Man-in-the-Middle (MiTM) attack occurs when attackers position themselves between a user and an internet server, intercepting the communication between them. This enables the attackers to eavesdrop on sensitive information shared by the user, such as addresses, passwords, or other personal data. For instance, a hacker may create a deceptive Wi-Fi network that appears free to access, enticing unsuspecting individuals to connect and unknowingly share their information with the attacker.

PROTECTING YOURSELF AND YOUR INFORMATION

While your organisation takes precautions against cyber-attacks (including cyber awareness training for employees), it's always beneficial to have your own cybersecurity strategies in place to protect your data at work, as well as in your personal life.

Back up your files: One effective measure to protect your data is to create backups on an online cloud server or an external hard drive, providing a crucial lifeline in case of unforeseen incidents. It's best to schedule backups and make it a habit of changing passwords to enhance security.

Report suspicious activity: If you come across a suspicious email, call, or text message, it is crucial to report it promptly. If your company has an IT or cybersecurity department, make sure to inform them about the incident. In cases where such a department does not exist, report the suspicious message directly on the platform through which you received it.

Don't access important information on public WIFI: Public WIFI is notoriously insecure, so think twice about using public networks before you use them to access personal or work accounts.

Stay vigilant: Employ strong, unique passwords for online accounts, utilise two-factor authentication, and be cautious about sharing personal information online. Regularly update privacy settings on social media platforms and exercise caution when interacting with unknown or suspicious sources.

WHAT SHOULD YOU DO IF YOU'VE BEED TARGETED?

We talk a lot about the importance of keeping yourself safe online, but we don't often talk about the personal fallout from experiencing cyber-crime. Several factors can influence a person's vulnerability, including:

- Online activities
- Mental health history
- Personal traits
- Attitudes toward technology

A victim of a cyber attack may lose more than money or dignity; they could also experience adverse psychological effects, such as anxiety or depression, shame and guilt, and reduced enjoyment of online activities they once trusted. In some cases, victims may experience symptoms of post-traumatic stress disorder (PTSD).

If you experience a cyber-attack at home or at work, it's crucial to identify and report suspect activity, but it can also help to talk to your loved ones about your experiences, and consider seeking the help of mental health professionals. As an employee, you have the option of speaking to your EAP for extra guidance and advice.

SECURITY TIPS FOR BUSINESS

There are a number of ways businesses can protect employees and customers practically.

Provide cybersecurity training: Boost employees' confidence in managing technology by offering basic cybersecurity training. This can include educating them on recognizing phishing and spam emails, creating strong passwords, and equipping them with tools to handle suspicious interactions. Consider integrating this training into the onboarding process for new hires or exploring online courses from platforms like Coursera and Udemy to educate employees on cybersecurity fundamentals.

FIND OUT MORE

1300 687 327 info@convergeintl.com.au convergeinternational.com.au

Converge INTERNATIONAL

Enable multi-factor authentication: Strengthen account security by implementing multi-factor authentication (MFA). Require users to verify their identity through an additional code sent via text or email, third-party authentication apps, or biometric features like fingerprints or facial recognition.

Improve access management for employees: Make use of identity management services such as Okta and 1Password to grant system access and application permissions to authorized users only. These services allow for specific permissions to be set per employee, ensuring better control over access.

Enhance employee engagement: In the wake of the COVID-19 pandemic, effective communication with employees is crucial. While concerns about remote work impacting productivity exist, prioritising employee happiness and implementing robust cybersecurity measures are equally important. Open channels for communication and create a supportive environment that values both productivity and cybersecurity.

FIND OUT MORE

1300 687 327 info@convergeintl.com.au convergeinternational.com.au

Converge INTERNATIONAL