

join the journey



HOODSWEENEY

Safety in the Technological Age

The importance of safety and protecting essential data

In the next 24 hours there will be more than 25,000 new malicious URLs uploaded with the goal of wreaking havoc on your online life. And this is just one type of threat.

These attacks pose a real danger and can gain access to any personal or business information entered online including; data, intellectual property and banking details.

Statistics from the US show that the average monetary loss of such incidences due to privacy breaches, time expenditure and cash theft is more than \$8,000 per incident.

So, can you afford not to protect yourself?

In this article, we explain the importance of safety and protecting essential data in a digital age.

Technology has made our lives easier in many ways we now have improved communications, time saving efficiencies, access to more information, automation and consistency.

It has seen the creation of a digital footprint for each individual which leads to a trail of information which can be accessed online. We also use technology for our personal banking, shopping and to stay in touch with friends.

Cyber criminals are excited about this wealth of information and it isn't a question of if but when you will be targeted.

There are a number of risks associated with having your life and business online such as; privacy breaches, ransomware, viruses, theft/fraud, data, intellectual property, money and identity theft.

When it comes to your business there are a number of ways you can mitigate these risks.

Business leaders must approach the cyber security challenge by looking at four important factors: people, process, technology and advice.

DISCLAIMER:

Information contained in this article is of a general nature only and does not constitute personal financial advice. The information has been prepared without taking into account your personal objectives, financial situation or needs. Before acting on any information in this article you should consider the appropriateness of the information with regards to your objectives, financial situation and needs. It is recommended specific financial advice be sought in relation to matters referred. The information in this document has been derived from sources we believed to be reliable and accurate. Subject to law, neither Hood Sweeney Accounting & Business Advisory ABN 30 007 696 595, AFS License No. 485569, nor their directors, employees, agents or representatives gives any representation or warranty as to the reliability, accuracy or completeness of the information; or accepts any responsibility for any person acting, or refraining from acting, on the basis of the information contained in this article.

People

Education and awareness for staff is the last line of defence when it comes to hacking and ransomware attacks.

Educate your staff to be vigilant when opening suspicious emails and any content that asks to open attached documents or click on web links.

Continue to update staff on the latest trends in cyberattacks and what to expect next. For example, the recent Origin Energy email which targeted consumers to pay their gas bill.

Encourage staff to challenge any material they receive that doesn't look right. Look at unusual wording and email addresses. Where will the link they want you to click on actually take you?

Process

Ensure you are conducting regular nightly, weekly and monthly backups to protect your essential data.

Conduct regular tests on multiple tapes and disks to ensure that the backups are working and your data and intellectual property is safe.

Backup processes can be the last line of recovery and have the ability to save organisations significant time and money when it comes to restoring systems.

Technology

There are a number of ways you can protect your technology from hackers or phishing.

Utilise anti-virus and anti-spam software as the first line of defence against threats to your systems and data.

Secure complex passwords and change them regularly and use encryption on all internet facing systems.

Always make sure your security patches are loaded and up to date.

Use unified threat management (UTM) as an addition to your traditional firewall to add layers of additional security.

Advice

Use an external IT expert to review your system independently to assess threats and risks to your business.

These professionals are equipped with specialist skills garnered over a number of years and have access to the most up-to-date information.

They will work with you to develop a plan to manage risks and allow you the peace of mind to focus on your business.

On another note

It is also important to consider cyber security at a personal level to protect yourself and your family.

Take note of how much information you are sharing online. Cyber criminals have been known to access online data such as; status updates and check-ins, fitness information and holiday snaps.

Emerging technologies means that those with sinister motives have the ability to take advantage of your digital footprint with real time information.

Why Hood Sweeney?

At Hood Sweeney we have significant experience in cyber security which can be tailored to your business and requirements.

We have specialist knowledge in a wide range of sectors and can adapt our experience to your needs combined with extensive knowledge of the security trends and advances in technology.

To learn more about the benefits cyber security could have for your business contact Technology Services Director Graham Wadsley on 1300 764 200 or email.

The Technology Services team at Hood Sweeney specialises in reliable, cost-effective and scalable solutions for information and communications, including:

- Tailored managed service agreements
- Planning for disaster recovery and business continuity
- Total solutions for mobile devices and communications
- Supporting your network and infrastructure
- Help desk and user support
- Procuring hardware and software.

For over 15 years, we've been helping clients across South Australia from private companies, publicly listed companies, government entities, not-for-profits and small-to medium-sized enterprises with hands-on operational support to put them on the right track with technology.



Graham Wadsley
Director

Technology Services
graham.wadsley@hoodsweeney.com.au