Security Awareness Implementation Guide

Stay Smart Online at all times

Being smart online is all about protecting sensitive corporate and customer information, your brand and your reputation, which are the most important assets your business will own. While every business is different, promoting safe online behaviour is critical, regardless of industry, state of the market or internal circumstances. Protecting yourself also protects friends, family and work.

To help your business stay safe and secure online, we have collated a few simple tips from businesses that effectively manage their information security risks.

Tips for improving employee awareness

This guide provides tips for businesses at a range of sizes and stages of developing information awareness and security programs. Some tips are more useful for businesses starting to develop their programs (Level 1), while others are more relevant to businesses taking advanced steps such as implementing cultural change to protect themselves and their workers (Level 2 - 3).

So whatever your size or budget, this guide will help you raise awareness of cyber safety within your organisation.

This guide has been developed by the Australian Government's Stay Smart Online Initiative in collaboration with the New Zealand Department of Prime Minister and Cabinet, Australia Post, Australia and New Zealand Banking Group Limited, Commonwealth Bank, NBN, National Australia Bank, Westpac and Telstra.

STAY SMART ONLINE

connect SMART
Protect yourself online

newzealand.govt.nz

Level 1 Start

- Ownership
- Personalise
- Resources
- Experiences

Level 1 – Getting Started

Situation: We're trying to establish the basics of online safety in our business. We're not IT savvy, have limited IT support, and don't have an awareness program in place. We're online mainly to process customer orders, read emails, and surf the internet. We don't have a big budget either!

Tips for keeping information safe

Take ownership

Assign responsibility for administering basic awareness around security. That person could be your office manager or if you are a sole trader, it's going to be you! When you hire new employees, you should train them in information awareness and security as part of their induction.

What's in it for me?

Make it personal. Provide employees with meaningful and relevant information about protecting their own lives and privacy. Good habits established at home will transfer to the workplace.

What is a strong passphrase? How can they spot suspicious messages or stop their identities being stolen? What are the key considerations for kids and teenagers' access to websites and apps? Once you have their attention, you can then link the information you provide back to a business context.

Take advantage of free resources!

Don't have a training budget? No problem. Free resources are available through the Australian Government's Stay Smart Online program and the NZ Government Connect Smart campaign.

- Give employees a copy of My Guide and talk about the eight steps in a team meeting[1]
- Encourage staff to subscribe to the Stay Smart Online Alert Service or follow the Facebook page for timely and actionable advice[2]
- Share the Small Business Guide with clients, suppliers or your small business peers and encourage them to talk to their staff about cyber security[3]
- Encourage employees to try the Connect Smart – How Cyber Smart are you? quiz[4]

Encouraging employees to check out this advice is another way to keep your business secure. Provide them with the links or resources and encourage them to put the advice into practice.

Share experiences

Share real life security incidents to highlight that information security incidents can happen to anyone, regardless of industry, age or background. Run an awareness-raising event in your workplace. You might also like to look at some examples on the Stay Smart Online YouTube channels. The New Zealand Connect Smart website also includes tips sheets with ideas and key messages. Have a conversation about the risks over a morning tea or during a team meeting.

[1] *Available from: https://www.staysmartonline.gov.au/myguide*
[2] *Sign up for Alerts at https://www.staysmartonline.gov.au/alert-service. Official Facebook page: https://www.facebook.com/staysmartonline*
[3] *Available from: https://www.staysmartonline.gov.au/smallbusinessguide*
[4] *Available from: https://www.connectsmart.govt.nz/home-users/cyber-smart-quiz*

STAY SMART ONLINE

connect SMART
Protect yourself online

newzealand.govt.nz

Level 2 Build

- Program
- Prevention
- Examples
- Relevance
- Situational
- Buy-in

Level 2 – Building on the Basics

Situation: My business has a dedicated IT person or services team, either in-house or outsourced. We manage customer data or have e-commerce functionality and know we need to get serious about being safe online. We have some ideas about how to implement an awareness program. To date, we have undertaken basic awareness activities, but want to improve.

If that sounds like your business, well done! Here's how to continuously improve the program

☐ **Have a program**

Have at least a basic security program in place. This may include simple measures such as simple calendar reminders or other tools to deliver security awareness messages or updates when and where you need to. Remember the bad guys don't take days off.

☐ **Prevention is better than cure**

In order for the message to stick and for employees to take action, awareness has to be part of how you run your business. Once-a-year training is not enough, so ensure your programs include regular, targeted messages. Regular newsletter articles, posters in visible locations, and desktop screen savers are all ways to keep the program visible all year round.

☐ **Use examples to illustrate the risks**

Not everyone is 'tech savvy'. Teach employees about the risks by drawing real life examples. If you're concerned about suspicious messages, make a comparison to real world examples to help the messages resonate.
For example, passwords or passphrases protect information in the same way that sunscreen keeps your skin safe and a PIN protects your credit card.

☐ **Keep it relevant**

Ensure that your awareness messages are current and relevant to your business and the technology it uses.
For example, you may highlight ransomware due to its rapid emergence as a threat over the past few years.

☐ **Take advantage of situations**

Throughout the year there are events that can be linked to online threats and risks to individuals and business.
For example, Valentine's Day is a prime time for an attacker to send false emails to people asking them to click on links or open attachments about collecting flowers. People who carry out these actions may be inadvertently infecting their computers with malicious software that locks files, captures information or spies on future activity. Another example is tax time, when attackers use logos and text to claim their malicious messages are actually from the Government. Ensure you use these opportunities to help raise awareness around security.

☐ **Board-level buy-in**

Treat cyber security as another risk that can impact all areas of your business, rather than just as an 'IT problem'.
Boards and directors must become comfortable with the challenge of understanding cyber-security risk across your business. Add a regular cyber security update to the agenda to raise visibility and understanding of cyber security issues at the highest level.

STAY SMART ONLINE

connect SMART
Protect yourself online

newzealand.govt.nz

Level 3 Mature

- Competitions
- Creativity
- Content
- Customers
- Suppliers
- Measurement

Level 3 – Culture Change

My business is seriously focused on security and manages risk at all levels of the organisation. Cyber security is understood as a whole-of-business concern and not just a problem for the IT department. We have executive-level support to continually improve our awareness program to manage risks, implement annual compliance training activities and to create a positive culture within the organisation to continue to improve the program.

Consider the following activities to help build on the positive culture within the organisation.

☐ **Get competitive**

Who doesn't like to win, right? Include rewards in your security awareness program. Create a competition on social media, or run a raffle at a team meeting or morning tea. Encourage employees to contribute ideas to ways the company's workforce can be safe online. Reward those employees who are proactive and highlight risks or threats before they become incidents.

☐ **Different folks, different strokes**

Depending on your business or location, you may need to consider different and creative ways of engaging employees who work out of the office, work shifts, or who are perhaps based in another country. Ways to connect with people on the move include Skype, webinars, and SMS alerts.

☐ **Customised content**

Your workforce is likely to be diverse, with each role carrying potential weaknesses that could be exposed in a security related incident. Ensure your content and messaging is customised to address a specific concern or risk. For example, you could tailor communications and training for application developers to ensure that they are actively involved in creating applications that are secure as well as functional.

☐ **Promote safe behaviour to your customers**

Use channels like social media to promote safe behaviour to your customers. If you're a retailer, you may provide safe online shopping tips. If you are a financial services business, you may highlight the risk to customers' online bank accounts of sharing passwords and using unsecured Wi-Fi networks.

☐ **Extend training to your suppliers**

Do your suppliers provide their employees with training? This is particularly relevant if they are managing any of your data. Work with your IT or information security contacts at your suppliers to ensure training programs are made available. You should also establish minimum security standards that each of your suppliers must comply with to retain your business, and validate compliance through audits.

☐ **Measure the results**

If your program is to be improved, it must be measured. For example, consider running an exercise where employees are sent a fake email to test whether safe online behaviours are being put into practice.

Conclusion

No matter how mature your business is regarding information security, you need to continuously improve and adapt your programs to a changing threat landscape. This means embedding awareness of good information security practices into the personal and professional lives of your employees, and staying abreast of developments in the area.

The emergence of ransomware in recent years shows that no business, regardless of size or industry sector, is immune from cyber threat. It's no longer just about the value of your data or customer information to malicious actors; it's about the value of that data and information to your own business. How would your business be impacted if all your files, contacts and software programs were locked? What are you doing to prevent your business being held to ransom?

Adopting a mature, dynamic approach to cyber security awareness can minimise the risk to your business of criminals gaining access to your corporate and customer information and using it for malicious purposes.

ISBN 978-0-9953944-2-1