User Security Awareness Training (USAT)

Program Outline

Even two raincoats may not keep you dry!

All businesses invest (sometimes significantly) in cyber security services and products which help to minimize their risks.

Like two raincoats, these cyber security measures **are not foolproof**. Even expensive titanium-plated security measures can be brought to its knees by a **hasty "click" or "download"**.

Your biggest risk – just so happens to be **your best line of defense**. Your users.

Carefully curated for NZ small business - our User Security Awareness Training (USAT) program is designed to help both yourself and your users become your "best line of defense".

We deliver this program to your users through:

- **Online:** This is a fundamental course included in most of our IT packages at no additional cost. The online course is run over a 12-month period (or depending on your preferences). It comprises around 32 short (<10 minute) courses with a focus on concepts, techniques and practices that offer the best protection to NZ small business.

- **In Person:** This will build onto the Online training concepts within small groups of ideally 6 or less to provide a collaborative session, real life examples and skill demonstrations.

Before, throughout and following up these courses – Millennium also provides your users with an easy way to report suspicious activity. Reporting incidents, and near misses, to the IT service desk will help us to better position your business and distribute information to keep your business safe.

Our Courses will run your users through the following:

- **Basics:** Go through the basics of internet safety and cyber security. Two short courses to introduce you to the concepts which we will dig deeper into.

- **Passwords:** A course that runs through the risks and provides real suggestions on how to implement better password practices.
- **Social Engineering:** Focuses on the methods attackers may use to "influence" us by basic human psychology. Awareness of these methods is key to Cyber Awareness.
- **Phishing:** A more expansive look at the most common type of social engineering. More than 90% of cyber-attacks in NZ start from a Phishing email – and often result in the attach becoming more complex and targeted.
- **Smishing & Vishing:** A short look into the use of social engineering techniques via Text Messages and Voice communications (such as phone calls).
- **Social Media Safety:** A look at some methods attackers might use via social media – and a reality check on what we should be putting on there. If you wouldn't put it on a billboard – don't put it on your social media.
- **Business Email Compromise:** Where someone poses as a supplier or other provider - and in many cases may have compromised a legitimate email address in order to create immediate trust with your users.
- **Malware:** Need no further explanation. This is bad stuff on your computer, tablet or mobile! But this course segment helps you learn some basics about it.
- **Privacy & Data Classification:** As a NZ small business - this is a straightforward and bite sized way to understand what sort of data you might want to protect.
- **Physical Security:** A look at shoulder surfing, tail gating, and the importance of physical security methods such as Lock Screens and Removable Devices.
- **Mobile Security:** A short segment about the importance of trusted WIFI and networks.
- **Executive Impersonation:** When someone like the Owner/Director/GM of your company contacts you to evoke an urgent response. They may not be who they say they are!