SECURITY AWARENESS AND EDUCATION WORKSHOP

COLLABORATIVELY USING BEST PRACTICE TO SECURE YOUR ORGANISATION

Security education and awareness programs are more likely to produce meaningful change when developed around clearly defined goals and a vision statement. In line with this, an NSP security awareness and education engagement will start with a strategic workshop

Strategic workshop - We will work with you to first identify a vision of your desired future state. Together, we will develop a raw list of the desired security practices you want to see embedded into end users' day to day actions, for example ' All end users use strong passwords' or 'End users use good security practices regardless of from where it is they are connecting to our systems and data.'

Continuous 12 month program - Continuous programs are known to more successfully reinforce learning by leveraging engaging and interesting content, simulated attacks and insightful communications. Rather than going to a lecture and forgetting it a week later, ongoing training presents employees with shorter learning bursts continually throughout the year. An effective security awareness training program should be both comprehensive and continuous - there is no end.

Measurable outcomes - Training attendance alone does not equal learning success. For a gauge on learning retention and behavioural change, which are more valid drivers for risk reduction, success measurement is critical. Regularly updated training with precise evaluation measurements is a must for keeping abreast of the ever-changing landscape of cyber awareness, so we will develop meaningful outcome-driven security awareness metrics by linking signature security behaviors to measurable operational outcomes.

Simulated attacks - A best practice security education program will intermittently test user knowledge via simulated attacks. As a result you will have visibility over users who require more training and who need more regular testing. We will work with you to identify the audience that will get these targeted phishing simulations, for example executive VIPs, privileged users and all staff.

WHAT YOU GET

Depending on the outcome of your strategic workshop, you will receive a training plan covering a selection of the following security topics

- CEO fraud prevention
- Phishing
- Ransomware
- Security awareness
- Social engineering
- Vendor risk management
- Password exposure