

SECURITY AWARENESS SERVICES

Security awareness is more important now than ever before. According to the Office of the Australian Information Commissioner (OAIC), in their first year of the Notifiable Data Breaches scheme, 62% of breaches were result of malicious or criminal attacks through phishing or compromised/stolen credentials. It takes just one inexperienced employee to not pick up on a slightly suspicious email for your business to fall victim. Your employees are the final human firewall to prevent potential targeted attacks.

CREATING EFFECTIVE SECURITY AWARENESS

We've seen customers fall down in their security awareness programs when key outcomes, business drivers and measures of success for the activity have not been identified. To be successful, security awareness needs to be addressed with a programmatic approach, not just as a one-time endeavour. For organisations with many priorities and limited resources, it can seem like a big project to tackle.



ASSESS CYBERSECURITY VULNERABILITIES AND RISKS

Before you start the process of educating your users it's helpful to know where you stand. By running a phishing simulation or short survey you can gather intel on the security awareness health of your business and act accordingly. Providing this hard data to your senior executives or business leaders can help to show why security awareness training is needed in the first place and gives you an honest, uncomplicated idea of improvements your business needs to make.



NOT EVERY ORGANISATION IS THE SAME

Once you have gathered insight into the state of your users' security awareness it's then important to identify your most vulnerable users. Cybercriminals will often target your Accounts team or high-value individuals such as CEOs, CFOs etc. So it's important that you understand their cybersecurity knowledge and if they require extra guidance and training.



TAILOR YOUR SECURITY AWARENESS CONTENT TO YOUR AUDIENCE

By tailoring the security awareness content to your audience, you will see greater success in your program. Users are more engaged when they are able to relate to the content and see how it connects to their everyday lives. Using short, succinct videos and training courses that are easy to consume and fit into busy schedules are far more effective.



TEST THE SUCCESS OF YOUR SECURITY AWARENESS TRAINING

Once users have undergone training it is important to measure the success of the program. This can be done testing the knowledge of your users with quizzes and running further phishing simulations to your organisation. This data can then be used as a comparison to your first benchmarking exercise and be presented to the senior executives of your business to show the effectiveness of your security awareness training.



RINSE AND REPEAT ON AN ANNUAL BASIS

Once these steps have been taken it's important that a cadence is set. InfoTrust suggests running this program on an annual basis, as cybersecurity threats are constantly evolving. It is also important as your user base may change year on year.



+61 2 9221 5555



www.InfoTrust.com.au



InfoTrust
Protection from Cybercrime

SECURITY AWARENESS SERVICES

InfoTrust offers a range of Security Awareness Services, including a comprehensive program of activities that can be rolled out in your organisation within 7 days and with minimum impact to your internal resources.

PHISHING SIMULATION-AS-A-SERVICE

Up to 4 fully managed campaigns over 12 months to test and educate your people around real email attacks seen in Australia. Run at 3-month intervals, these campaigns give you and your executive team insight into the effectiveness of the program and show how security awareness improves across your organisation

TARGETED SECURITY AWARENESS CONTENT

InfoTrust provides organisations with ready-to-use security awareness content that addresses key issues. From boards and executives, to developers and end-users, InfoTrust has a catalogue of videos and SCORM packages that can be deployed in your organisation's learning management system or Intranet.

SECURITY AWARENESS STRATEGY

Not every organisation is the same, and every employee learns in a different way. InfoTrust works with you to create a program of work to raise organisational awareness programmatically using a multi-thread approach that covers all learning styles.

EXECUTIVE REPORTING

Benchmark your organisation's security awareness and measure improvements. These executive reports also give you tangible results you can report to your senior management to showcase the need and return on investment for running security awareness programs.



EMPOWER YOUR EMPLOYEES TO BE MORE SECURE

INFOTRUST ADVANTAGE

InfoTrust has worked with many organisations to create bespoke security awareness programs that aid them with compliance, and mitigating the risk from targeted email attacks. Our email security experts have unique insight into the most common socially engineered attacks that are happening in Australia today and are able to test your end-users' preparedness for these.

 +61 2 9221 5555

 www.InfoTrust.com.au



InfoTrust
Protection from Cybercrime