

*Protect your employees and remote workers from emerging email threats by teaching your staff to identify and respond to potential security risks.*



## Solution Overview

One of the biggest liabilities to an organisation's security starts at the frontline – not with your IT, but your employees. According to Gartner Inc., 95% of data breaches are caused by human error, with 91% of cyber attacks starting with a phishing email. Ensure your organisation has the best frontline defence with our fully-managed phishing awareness and training program. Measure your organisation's vulnerability towards phishing attacks in a safe and controlled environment, whilst training your organisation to be cyber security conscious.

Benefits of our fully-managed email phishing simulation and training program:



### Simulate and Test

Real-world phishing templates are periodically sent from a vast threat database, exposing your users to the latest email threat types.



### Analyse and Report

Detailed metrics on user behaviour is tracked to recognise security risks and develop the best training approach.



### Educate to Mitigate

Training track is chosen from a large variety of engaging content, designed to address your specific vulnerabilities.



### Repeat for Retention

Success is tracked and measured for the next term of testing. Continuous training is most effective at influencing user behavioural change.

To learn more about how our IT services can help drive your business, call **1300 705 062**, email us at [sales@abtechnologies.com.au](mailto:sales@abtechnologies.com.au), or visit our website at [www.abtechnologies.com.au](http://www.abtechnologies.com.au).

## ABT Corporate Snapshot

We are a member of the ASCS - Managed Service Provider Partner Program (MSP3), which is part of the Australian Signals Directorate's Australian Cyber Security Centre (ACSC) that provides expert guidance to help entities mitigate cyber security incidents caused by various cyber threats. Our accreditations include ISO 9001:2008 Quality Assurance, GISC Accreditation Q-2645.



## Key Focus Areas



### Simplify security awareness



A full security awareness program with proven curated testing and training content, and efficient, automated reports all in one customized package.



### Meet compliance requirements



When security awareness and training requirements are mandatory, make it easy for your organization to meet regulations, fight security risks, and stay secure with a ready-to-launch training program.



### Gain real insights to vulnerabilities



Thousands of data points have been captured to provide you a deeper and more useful insight into exactly where your risks exist within your organisation. This way we can precisely target the awareness programs towards your users using user-behaviour metrics, detailed trend analytics, benchmark statistics, and customisable reports and dashboards.



### Education on all email threat types



Research based on real-time threat intelligence has identified 13 key types of email threats. It is our job to help your users understand the nature and characteristics of these 13 threat types, to build the best protection for your business, staff, and data.



### Comprehensive email security



Email awareness and training combined with our multi-layered email security solution, offers to eliminate the stress of support headaches with other multi-vendor solutions.

## 1 Simulate and Test

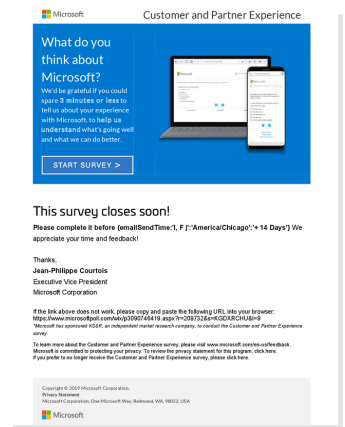
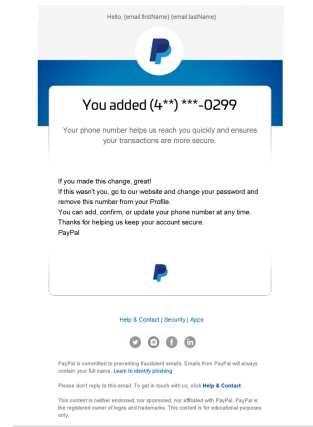


A full security awareness program with proven curated testing and training content, and efficient, automated reports all in one customized package.

Real-world phishing templates are periodically sent from a vast threat database, exposing your users to the latest email threat types.

### Features:

- 8 simulation campaigns per year
  - Over a 2 week period with emails sent to all recipients at random times during this period.



## 2 Analyze and Report



Thousands of data points have been captured to provide you a deeper and more useful insight into exactly where your risks exist within your organisation. This way we can precisely target the awareness programs towards your users using user-behaviour metrics, detailed trend analytics, benchmark statistics, and customisable reports and dashboards.

### Features:

- Detailed reports sent to the nominated contacts at the end of each campaign showing click rates, credentials phished, etc.

### Results Summary

This Training Campaign ran from 10/11/2020 to 10/12/2020 and data collected through 10/19/2020.

- Total Emails Sent: 1
- Users Who Replied to Email: 0
- Users Who Started Training: 1 (100%)
- Users Who Completed Training: 1 (100%)
- Users Who Reported Email as a Potential Phish: 0



## 3 Educate to Mitigate

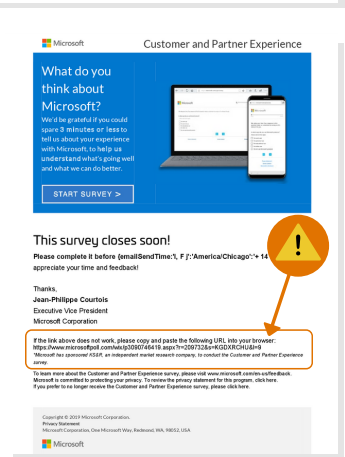
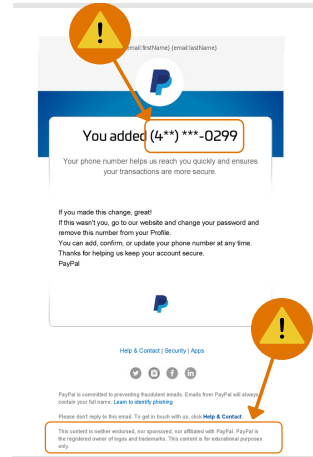


Training track is chosen from a large variety of engaging content, designed to address your specific vulnerabilities.

Research based on real-time threat intelligence has identified 13 key types of email threats. It is our job to help your users understand the nature and characteristics of these 13 threat types, to build the best protection for your business, staff, and data.

### Features:

- 4 training campaigns per year
  - Data-driven short videos & quizzes based on the results of previous simulation & training campaigns.



## 4 Repeat for Retention



Success is tracked and measured for the next term of testing. Continuous training is most effective at influencing user behavioral change.

When security awareness and training requirements are mandatory, make it easy for your organization to meet regulations, fight security risks, and stay secure with a ready-to-launch training program.

### Features:

- Detailed report at the end of each training campaign outlining who has watched the video (or ended prematurely), and the number of attempts for the quizzes.

