Why should you invest in security awareness training?

Ransomware, fraud and data breaches that's why . . .

Username

Password

Login
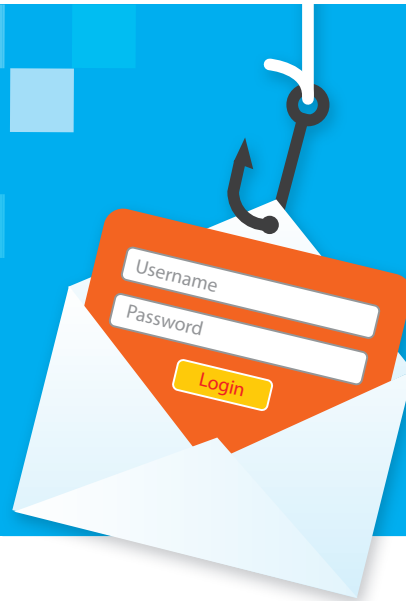
One of the greatest threats to information security could actually come from within your company, often it is the non malicious, uniformed employee.

Did you know that 91% of successful data breaches started with a phishing attack?

What is Phishing?

Phishing is when a criminal attempts to obtain sensitive information by pretending to be someone else or a reputable company. Most often this is via email but could also be via text or a phone call.

How can it effect my business?

Reputational damage, loss of custom, loss of money, business disruption and data breaches can be the result of a successful phishing attack.

These threats are on the rise because they are extremely profitable and users are exposed to increasingly more sophisticated social engineering threats everyday.

How can I protect my business?

One of the best ways to make sure company employees will not make costly errors in regard to information security is to institute company-wide security-awareness training campaign.

NCI have partnered with an innovative provider of security awareness training, and can delivery an automated training and simulated phishing campaign that will continually educate your staff and build a more resilient and secure organisation.

How it works

Phish your users

Your end users use LinkedIn, Twitter, Facebook, Amazon, Office 365, Dropbox, Google. And these well-known platforms are known to be used in phishing attacks.

We will run best-in-class simulated phishing attacks on your users, this is an automated email campaign that uses email templates of real world attacks. It is completely safe and will highlight who is susceptible to phishing and can auto enrol those users in more targeted security awareness training.

Your users are the last line of defence
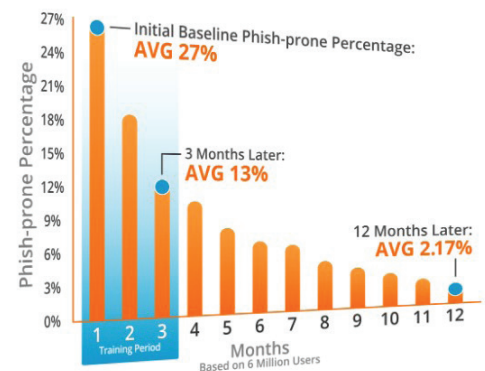
Train your users

An automated campaign of security awareness training is run via email. This includes web based training such as short videos, posters, interactive modules and newsletters from the world's largest library of security awareness training content. Content can be targeted for example to staff working in finance, education, healthcare or customer service and includes more than 50 topics such as Common Sense, GDPR, Cyber Crime, Compliance, Data Breach, Email Security, Sensitive Information, PCI etc. This training is completely automated with scheduled email reminders and reporting.

Security Awareness for New Hires

Published: Jan 14th, 2019
Category: Training Modules
Duration: 10 mins

Learn more...

SECURELY WORKING FROM HOME

Executive Series: Securely Working From Home

Published: May 16th, 2019
Category: Video Modules
Duration: 2 mins

Learn more...

See the results

Simple reporting shows stats and graphs for both training and phishing. Reporting will show who is susceptible to phishing and the status of each individuals training.

When you send simulated phishing and training campaigns to your employees on an ongoing basis they learn to STOP, LOOK, and THINK before they click. You are training your employees to be part of your defence strategy and they are active participants in helping to protect your organization's risk to social engineering.

Initial Baseline Phish-prone Percentage:
AVG 27%

3 Months Later:
AVG 13%

12 Months Later:
AVG 2.17%

Based on 6 Million Users