Cybersecurity Awareness

KELTY
BUSINESS SOLUTIONS

15 Ways To
Protect Your Business From A Cyber Attack

DID YOU KNOW?

1 in 5 Small businesses will suffer a cyber breach this year.

81% of all breaches happen to small and medium-sized businesses.

97% of breaches could have been prevented with today's technology.

Protect your income and business with these tips!

SECURITY ASSESSMENT

It's important to establish a baseline and close existing vulnerabilities. When was your last assessment?

SPAM EMAIL

Secure your email. Most attacks originate in your email. We'll help you choose a service designed to reduce spam and your exposure to attacks on your staff via email.

PASSWORDS

Apply security policies on your network. E.g. Deny or limit USB file storage access, enable enhanced password policies, set user screen timeouts and limit user access.

WEB GATEWAY SECURITY

Internet security is a race against time. Cloud-based security detects web and email threats as they emerge on the internet, and blocks them on your network within seconds - before they reach the user.

ADVANCED ENDPOINT SECURITY

Protect your computers and data from malware, viruses, and cyber attacks with advanced endpoint security. The latest technology (which replaces your outdated anti-virus solution) protects against fileless and script-based threats and can even roll back a ransomware attack.

MULTI-FACTOR AUTHENTICATION

Utilize this on your network, banking websites, and even social media. It adds an additional layer of protection to ensure that, even if your password gets stolen, your data stays protected.

COMPUTER UPDATES

Keep Microsoft, Adobe, and your other products updated for better security. We provide “critical update” service via automation to protect your computer from the lastest known attacks.

DARK WEB RESEARCH

Knowing in real-time what passwords and accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach. We scan the Dark Web and take action to protect your business from stolen credentials that have been posted for sale.

SIEM/LOG MANAGEMENT

(Security Incident & Event Management) Uses big data engines to review all event and secuity logs from all covered devices to protect against advanced threats and to meet compliance requirements.

Encryption

Whenever possible, the goal is to encrypt files at rest, in motion (think email) and especially on mobile devices.

FIREWALL

Turn on Intrusion Detection and Intrusion Prevention features. Send the log files to a managed SIEM.

MOBILE DEVICE SECURITY

Apply security policies on your network. E.g. Deny or limit USB file storage access, enable enhanced password policies, set user screen timeouts and limit user access.

BACKUP

Backup local, Backup to the Cloud. Have an office backup for each month of the year. Test your backups often.

SECURITY AWARENESS

Train your users - often! Teach them about data security, email attacks, and your policies and procedures. We offer a web-based training solution and “done-for-you” security policies.

EXTRA PROTECTION

If all else fails, protect your income and business with cyber damage and recovery insurance policies.

WHY IS TRAINING IMPORTANT?

10-15% of phishing attacks make it through your security filters. In a study of nearly nine million users across 18,000 organizations over a 12-month period, it was found that an initial baseline of 30% of all industries were phish-prone. After only 90 days of security training and simulated phishing, this percentage dropped to 15% and was minimized to only 2% after one year of training – an astounding 92% improvement.

Employees are the first line of defense for an organization. It's important to enable your employees to make smarter security decisions by training them to understand the mechanisms of spam, phishing, spear phishing, malware, ransomware, and social engineering, and then get them to apply this knowledge daily. Our Online Security Awareness Training program is meant to be a tool (in addition to quality spam filters, firewalls, and/or anti-virus) as part of a defense-in-depth strategy. We will prepare your users to better defend your organization against cyber attacks and manage problems that arise when attacks make it past your other defenses.

Kelty iManagement is equipped to provide you with a detailed and customized security plan for building a strong human firewall as your organization's last line of defense.

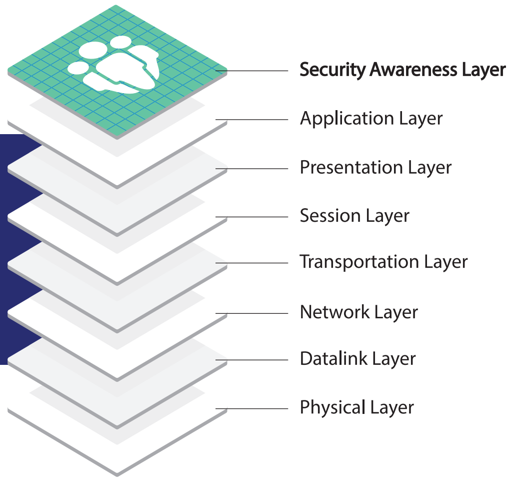
$26 BILLION CEO Fraud (aka Business Email Compromise) exceeded $26 billion in damages

91% of successful data breaches started with a spear hishing attack

34% of businesses hit with malware take

75% of companies infected with ransomware are running up-to-date endpoint protection

People are a critical layer within the fabric of our Security Programs



KELTY
BUSINESS SOLUTIONS

CYBERSECURITY

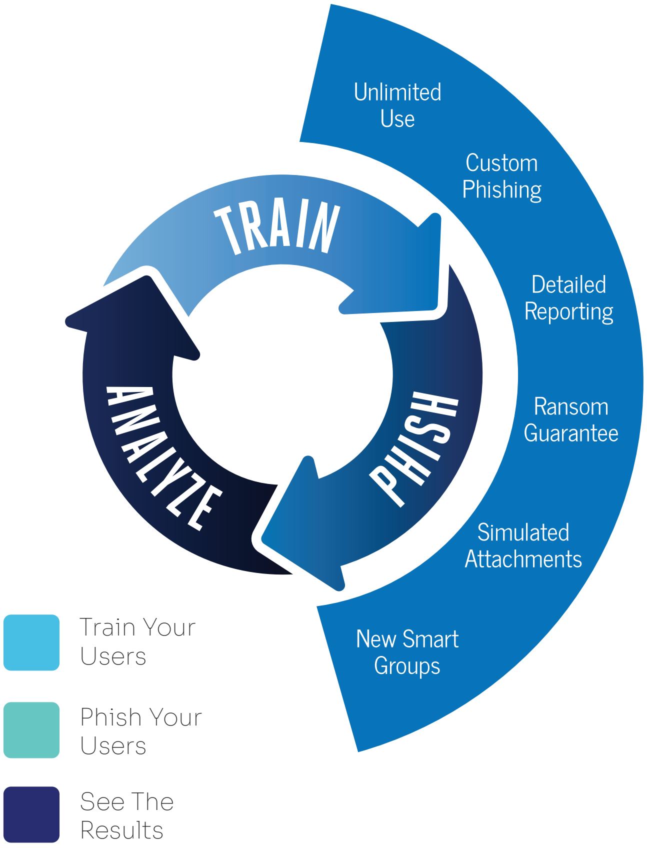
OUR THREE-STEP PROCESS

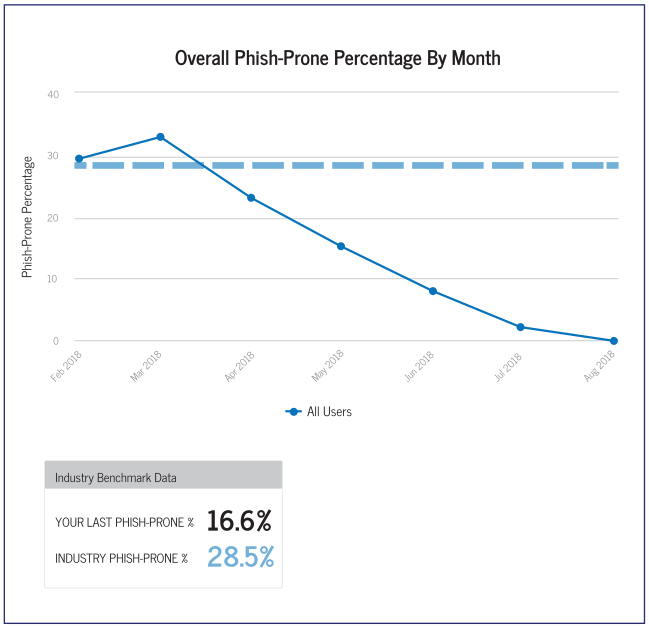
Through the Online Security Awareness Training program, we follow three steps to create a foundation of security for your organization.

1. Determine Phish-Prone Percentage. A baseline phishing test will determine your organization's phish-prone percentage. Kelty iManagement will set up whitelisting, email merge, analyze the report that is generated from this test, and make recommendations for training.

2. Assess Security Awarenesss. We will set up a security awareness survey for your employees to take, assess the current knowledge and assign training based on the results. Training campaigns will be built and reports will be made based on your employees' progress. Training certificates for each employee will be sent to your HR department for their files. Showing ongoing training is a necessity for compliance.

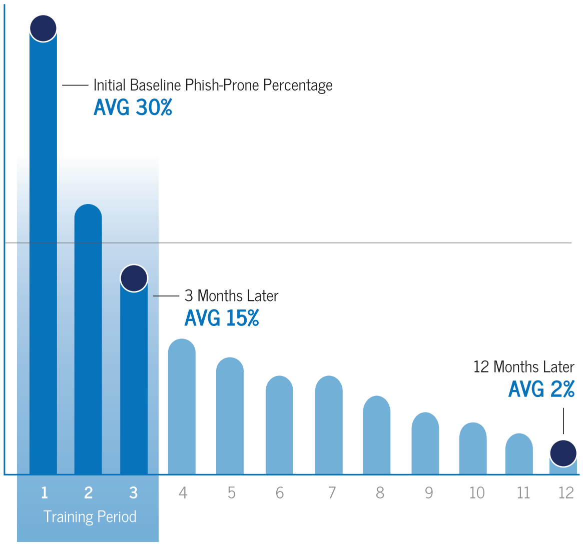
3. Ongoing Training. We will set up ongoing phishing and training campaigns to allow your users to practice the skills they've learned in their security awareness training. From the responses we will compile and analyze reports. To keep your users security-focused, we assign a new course quarterly to keep your users engaged in their security awareness training and to keep the content fresh.

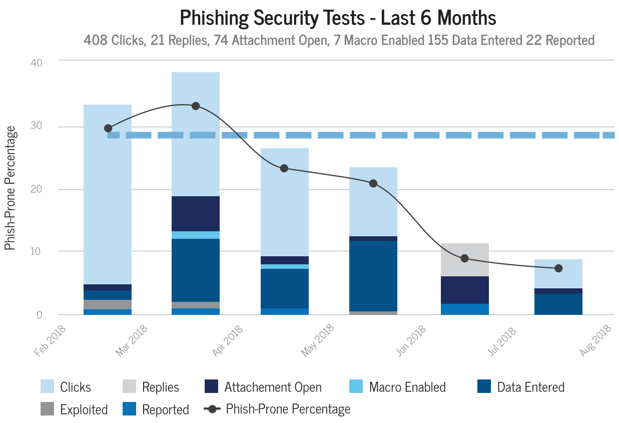




Industry Benchmark Data

YOUR LAST PHISH-PRONE %	16.6%
INDUSTRY PHISH-PRONE %	28.5%





Industry Benchmark Data

YOUR LAST PHISH-PRONE % **7.9%**

INDUSTRY PHISH-PRONE % **28.5%**

In addition, we also have built-in Security Hints and Tips and a Scam of the Week to help build online security awareness. Security Hints and Tips will remind users of various general methods of how to stay safe online and at work. Scam of the Week will prepare your users to defend themselves against the latest cyber security attack and social engineering scams.

We will review the various reports to see your organization's progress over time. Analyzing the various reports available to you may help you to shape future plans for phishing tests or security training campaigns by revealing "weak links" in the organization, where a heavier focus on security training may be required.

This plan will constantly remind your employees to keep security in mind and we strongly recommend this plan for any organization that handles sensitive information.

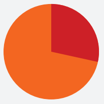
Generating Industry-Leading Results and ROI

- ↓ Reduced Malware Infections
- ↓ Reduced Data Loss
- ↓ Reduced Potential Cyber-Theft
- ↑ Increased User Productivity
- ↑ Users Have Security Top of Mind

127 % ROI WITH ONE-MONTH PAYBACK

Report Date: 2020-03-13
Email: john.doe@keltysolutions.ca
Domain: keltysolutions.ca
Organization Size: 17

88% EXPOSED



11 | 4 Identities Found | 15 Unique Breaches

VERY HIGH RISK	✓ DATA FOUND	✓ BREACH	✓ PASSWORDS
Emails: 3		Indentities: 0	
HIGH RISK	✓ DATA FOUND	✓ BREACH	
Emails: 8		Indentities: 4	
MEDIUM RISK	✓ DATA FOUND		

KELTY
BUSINESS SOLUTIONS

Kelty iManagement Head Office
301-10th Street, Brandon,
MB R7A 4E9 p
h. 204.726.0242

Kelty iManagement Steinbach
316 Main Street, Unit A
Steinbach, MB R5G 1Z1
ph. 204.326.1085

keltysolutions.ca