ISA INFINITY

PARTNER BATTLE CARD: Selling SOC-as-a-Service **TRAIN** (Security Awareness)

Train your client for phishing attacks

You know phishing is a threat, but do you know the facts?

Although automated email security tools are continuously improving, many phishing and spear phishing attacks are successful in bypassing them. Employees play a vital role, so good security behaviors are a critical line of defense to protecting an organization and can only be achieved through an engaging, effective security awareness training program.

Phishing is at the highest level in years and is the primary infection vector used by malicious actors*

Only 26% of phishing is stopped by technology alone and 38% of employees fail a phishing test°

On average, after 1 year of on-going training with **TRAIN**, less than 5% of employees fail¤

ISA TRAIN, Security Awareness as a Service.

Our state-of-the-art Security Awareness program, **TRAIN**, engages clients' employees, instilling confidence that they can successfully recognize and report a potential security threat, thus preventing it from becoming a security breach. ISA's proven strategy provides actionable data on employee susceptibility to phishing attacks by identifying employees who may need additional help in strengthening their security behaviors.

ISA's "Train, Phish, Analyze, and Repeat" Strategy.

By analyzing click-rates on phishing emails both before and after training modules are implemented, business leaders can see a measurable metric of the impact that a training and phishing campaign has had on their employees' security awareness. Using **TRAIN**, specific departments that may be more susceptible to certain types of high-risk phishing attacks, can be spear phished, using customized campaigns.

.

*According to APWG's Phishing Activity Trends Report for Q3 2019 (apwg.org, 2020) °According to the 2018 Cisco Cybersecurity Report) ¤Cybersecurity Skills Shortage Soars, Nearing 3 Million (isc2.org, 2018) †ISTR Internet Security Threat Report Volume 24 (Symantec, 2019)

What is Phishing and Spear Phishing?

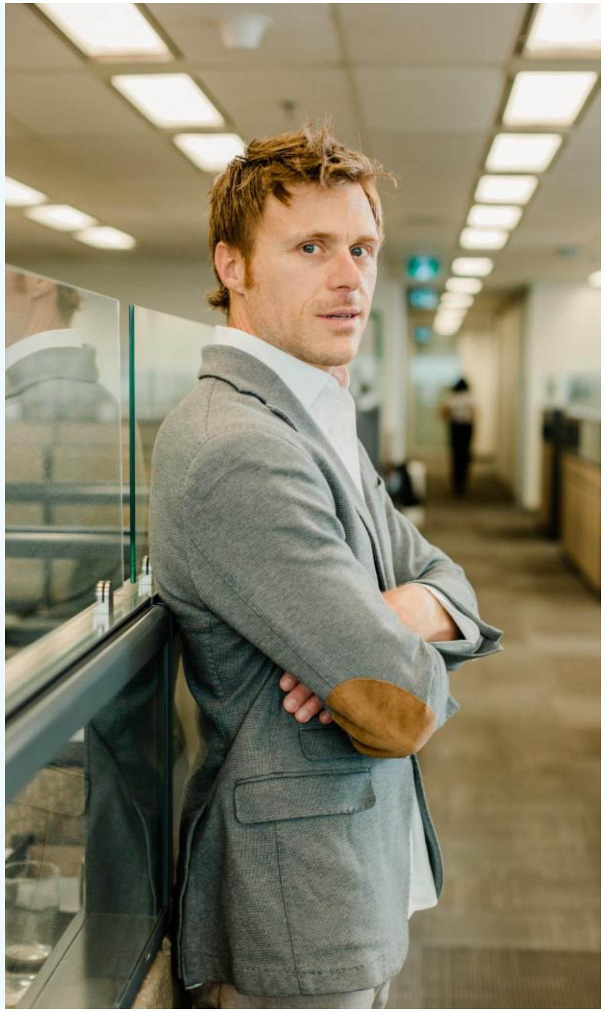
Phishing is a cyberattack by sending a malicious email that tricks users to surrender their user credentials or perform a malicious action, like downloading unauthorized software. The email may appear legitimate, as if coming from an internal employee, a business partner, the user's bank, etc. Often, the mail will ask you to reset your password.

In a spear phishing attack, an individually-crafted email targets a key executive or decision maker. Spear phishing emails are used by almost two-thirds† of all known groups carrying out targeted cyber attacks.

Our approach:

Delivered through ISA's 24/7 by 365 monitored, SOC 2 Type II certified Cyber Security and Operations Centre (CIOC), **TRAIN** is separated into four distinct areas:

+ We provide **BASELINE TESTING** to assess the phish-prone percentage of your users through a simulated phishing attack.
+ We **TRAIN** your users, leveraging a library of over 1000 training assets, including interactive modules, videos, games, posters, newsletters, and scheduled reminder emails.
+ Through best-in-class simulated attacks, using hundreds of standard templates that can be customized, we **PHISH** your users.
+ Actionable insights are provided through exhaustive **REPORTS**, showing statistics and graphs for both training and phishing.



ISA INFINITY

PARTNER BATTLE CARD: Selling SOC-as-a-Service **TRAIN** (Security Awareness)

Starting the conversation for Security Awareness as a Service

Conversation starters for ISA TRAIN:

CEO, CIO, and CISO:

- How confident are you that your employees are properly trained to spot and flag a phishing email?
- How are you currently improving your employees' security awareness?
- Do you know your organization's current Phish-Prone Percentage?
- Are you interested in an outcome-based security awareness and/or training solution as a service?

IT Director:

- Does your team have the expertise to detect and respond to phishing threats?
- What industry regulations do you need to comply with? How do you report on your cybersecurity posture?
- Do you currently have a training program in place; how often is it updated?
- Is Security Awareness part of your employee on-boarding?

IT Specialist:

- How much time do you spend setting up your current Security Awareness training program?
- How often do you currently test your users on Security Awareness?
- How many employees are currently failing your Security Awareness testing?

Here are 6 reasons why Canadians are choosing ISA services:

IDC MarketScape©: "ISA is a Major Player in Canadian Security Services."‡

ISA is Canada's largest pure-play Managed Security Services Provider

ISA has offices across Canada and guarantees Canadian Data Residency

ISA has a culture built on quality, commitment and integrity*

ISA's state-of-the-art CIOC is SOC 2 Type 2 certified by AICPA

ISA is recognized as a top partner by industry leading technology vendors°

‡https://www.idc.com/getdoc.jsp?containerId=prCA45450419 *Articulated as such by the ISA Client Advisory Council. °Visit the ISA website for partnership details.

Learn more about the ISA Infinity Partner Program at www.isacybersecurity.com/cn-partners-infinity | Register a deal via infinity@isacybersecurity.com | Contact Ingram Micro for more information via CyberSecurityCanada@ingrammicro.com

INGRAM MICRO®