Canon
CANON SOLUTIONS AMERICA

Barracuda® PhishLine

SECURITY AWARENESS TRAINING
AND SIMULATED PHISHING PLATFORM

CANON SEE IMPOSSIBLE

PEOPLE – YOUR WEAKEST LINK, OR YOUR BEST DEFENSE?

EXECUTIVE SUMMARY

When it comes to threat mitigation, the reality is that your people are either the weakest link that cyber criminals are looking to exploit through social engineering, or they can be your best defense if they are made aware in a consistent manner and in a meaningful way.

There is no more important element in a successful security posture than employee awareness. Some of the most catastrophic data breaches in recent history were the result of an insider being exploited by an email phishing attack.

WHAT IS PHISHING?

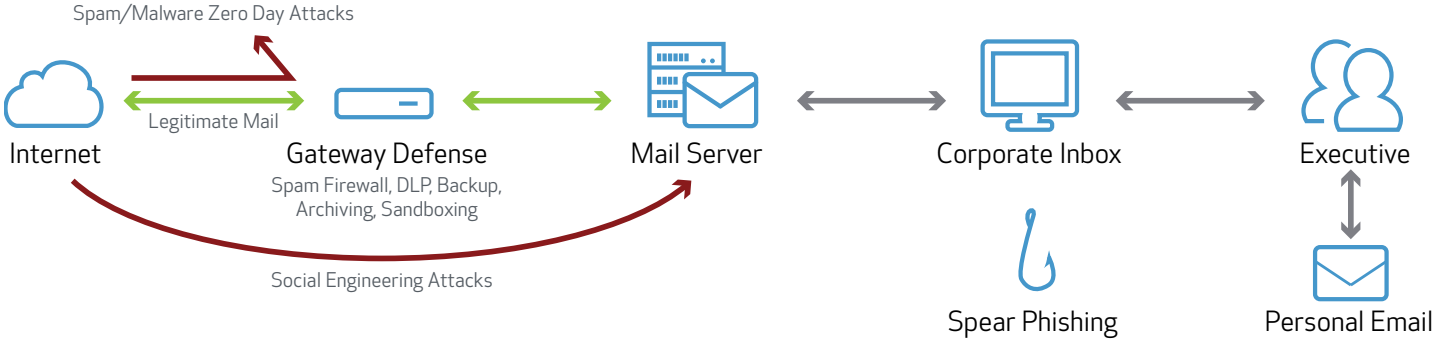
Phishing is a technique used by hackers to impersonate a trustworthy entity in an email. Attackers use phishing emails to obtain sensitive information such as usernames, passwords, or banking credentials. They distribute malicious links and attachments to trick users into downloading malware or ransomware. These attacks are usually sent in large numbers to business users and consumers—more or less at random—with the expectation that only a small number will respond.

THE BARRACUDA ADVANTAGE

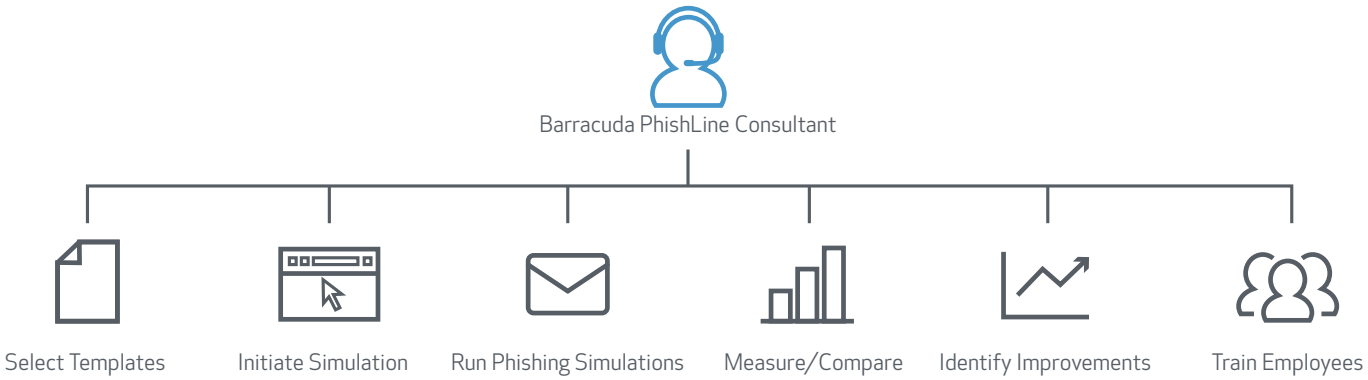
- Protect your business with a versatile, scalable, cloud-based SaaS solution
- Guard against a range of threats with patented, highly variable attack simulations for Phishing (Email), Smishing (SMS), Vishing (Voice) and Found Physical Media (USB/SD Card)
- Train users with comprehensive, SCORM-compliant courseware
- Get industry-leading analytics and reporting
- Take advantage of program and address book automation

PRODUCT SPOTLIGHT

- Choose from hundreds of email templates, landing pages and domains
- Automatically direct training and testing with the built-in workflow engine
- Make it easy for users to instantly report suspicious emails with the Phish Reporting Button
- Embed learning into your everyday business processes
- Test and reinforce good behavior



Let Barracuda email security experts run your PhishLine simulation campaigns for you.



PHISHLINE CONCIERGE SERVICE

PhishLine Concierge is an optional premium service that offloads the tasks of defining, configuring, executing, and analyzing your phishing simulation campaigns to a dedicated Barracuda email security expert. Your PhishLine Concierge expert consultant can give you a complete, managed-service experience, running every aspect of your security awareness training. Or you can choose to engage more actively as a partner in creating and executing custom phishing simulation campaigns. Concierge Service includes:

EXPERT CAMPAIGN DESIGN

Your PhishLine Concierge consultant has the expertise to design high performance, SCORM-compliant training programs that leverage the latest developments in the field of automated, computer-based learning. With access to Barracuda's global, real-time threat intelligence network, they ensure campaigns are relevant to the latest trending threats based on your region, size, industry, and more.

EXPERT CAMPAIGN OPERATION

Your Concierge consultant delivers complete, turnkey operation of your campaigns from beginning to end. By leaving your security awareness training in the hands of an experienced, knowledgeable security-training expert, you free up resources to attend to your day-to-day operations.

EXPERT CAMPAIGN RESULTS

Customers who use Concierge Service consistently report double digit phishing awareness improvements across a broad range of departments and employees. PhishLine's advanced metrics and reporting capabilities let you easily measure your users' improvements, and identify individuals and departments that require advanced security training.

TOP 3 PHISHING ATTACKS

And How to Defend Against Them

PHISHING

WHAT IS PHISHING?

Phishing is a technique used by hackers to impersonate a trustworthy entity in an email. Attackers use phishing emails to obtain sensitive information such as usernames, passwords, or banking credentials. They distribute malicious links and attachments to trick users into downloading malware or ransomware. These attacks are usually sent in large numbers to business users and consumers—more or less at random—with the expectation that only a small number will respond.

HOW TO BLOCK PHISHING ATTACKS

Anti-phishing solutions use a combination of techniques to detect and prevent phishing attacks. They check the reputation of the domain and sender, see if a sender or link within an email was used in previous phishing campaigns, scan websites for malicious downloads, add link protection to block links that may become malicious over time, and compare the body of the email to previous messages that were categorized as malicious.

SPEAR PHISHING

WHAT IS SPEAR PHISHING?

Unlike mass phishing attacks, spear-phishing emails are carefully designed for a specific individual to get them to respond. Attackers invest time in researching these individuals and their organizations to craft a personalized message, and only send very few messages at a time. These attacks come from high reputation sender addresses or already compromised accounts and often contain zero-day, never used before links that don't appear obviously malicious to most security protection solutions. Hackers rely on these highly effective spear-phishing attacks to steal credentials or infect devices with malware.

HOW TO BLOCK SPEAR PHISHING ATTACKS

Spear-phishing attacks often are able to bypass traditional security gateways, which mostly rely on reputation analysis, blacklists, and look for malicious payloads. To block spear-phishing attacks, a security solution needs to include an intelligent, context-aware technology to identify anomalies in the content of the email. These anomalies can include mismatch between sender identity and email address, expressions commonly used in phishing attacks, suspicious call to actions, and links that are anomalous to the context of the email.

BUSINESS EMAIL COMPROMISE

WHAT IS BUSINESS EMAIL COMPROMISE (BEC)?

BEC attacks—also known as CEO fraud, whaling, or wire transfer fraud—impersonate an employee within the organization in order to defraud the company, its employees, customers, or partners. In most cases, attackers will focus their efforts on employees with access to the company's finances or personal information and trick individuals to perform wire transfers or disclose sensitive information. These attacks utilize socially engineered tactics, compromised accounts, and often have no attachments or links.

HOW TO BLOCK BEC

Similar to spear phishing, relying on an email gateway is not enough to detect and block BEC. Organizations need technology that does not rely on static rules to detect these targeted attacks, rather a solution that provides analysis of its historical communication patterns and visibility into internal email communication. This helps to determine with a higher degree of accuracy whether a certain email is part of a BEC or account takeover.

Canon

CANON SOLUTIONS AMERICA

For more information, call or visit
800-815-4000 CSA.CANON.COM/SECURITY

1/19-083-3045