Advanced Persistent Testing:

How to Fight Bad Phishing with Good.

PhishLine®
Measured Security Awareness

Written by: Mark Chapman

Table of Contents

Targeted Threats Increase Risk

PhishLine®
Measured Security Awareness

Targeted Threats Increase Risk

“Spam” used to be a quantity-over-quality endeavor. An attacker would simply send out a few hundred thousand not-so-carefully-crafted emails and hope a few percent of the victims would ultimately part with their money.

Today, the threat is much more targeted and much more sophisticated. Spear-phishing, Whaling and other terms describe the techniques of targeting emails and other messaging to specific organizations or individuals to invoke harm.

- **Financial Loss** - Various sources place the annual economic costs of traditional phishing at over $3B. It is difficult to estimate the non-reported or undetected enterprise-level losses.
- **Reputation Damage** - There are several high-profile instances where trustworthy enterprises experienced reputation damage due to phishing.
- **Technical Breaches** - Phishing attacks are often used to gain unauthorized access to systems. Advanced malware aside, it is often easier to simply trick someone into sharing a password than to directly hack the technical controls.
- **Strategic Harm** - It is hard to estimate the harm when a phishing attack leads to disclosure of valuable competitive or other strategic information.

Why Targeted Attacks are Effective

PhishLine®
Measured Security Awareness

Why Targeted Attacks are Effective

Targeted attacks greatly increase effectiveness by exploiting security vulnerabilities in people, process, and technology. Determined attackers leverage combination attacks where an exploit on one attack vector may lead to another for a particular target.

People

Historically, the “human firewall” component is generally thought to be the weakest security link. Con artists exploit natural human tendencies, like curiosity and the desire to be helpful, to perform effective social engineering attacks.

Today, people have limited time, ability, and motivation to validate the authenticity and intent of most electronic communications. If a seemingly innocuous message is somewhat compelling, some subset of users will inevitably interact by opening the message, replying, clicking on links, and sharing information.

To help prevent social engineering attacks, security awareness training is paramount. Measuring the success of that training and targeting appropriate follow-up training is an ongoing challenge.

Process

Phishing attacks can exploit vulnerabilities in certain processes such as incident response, support escalation, or disaster recovery.

One approach is to launch a bold and unsophisticated phishing campaign to cover up a lower profile attack or to cause other harm. For example, attackers may temporarily shut down the benefits department by sending out a notice that all employees will soon lose their benefits.

Careful proactive testing of incident response processes will help organizations reduce the potential side effects of malicious social engineering attacks. The lack of automated testing solutions limits the quantity and quality of process-based testing in many organizations.

Technology

Attackers target the technology vector because that is where the valuable confidential information is transmitted, processed, and stored.

There are many advanced controls to limit the impact of technology vector attacks including anti-malware, intrusion prevention, patch management, and Data Loss Prevention (DLP) solutions. These controls defend against well-known attack methods including advanced malware and exploitation tools triggered through malicious phishing campaigns.

The basic limitations of these controls are fairly well understood. “Zero-day” attacks are one example where vulnerabilities are exposed before patches are available. Limited coverage on non-enterprise owned devices is another well-known limitation.

In many organizations, the effectiveness of technology vector controls are by far the most well understood. It is sometimes a challenge to validate without actually introducing malware or deploying intrusive probes on non-enterprise devices.

Layered Defense

PhishLine®
Measured Security Awareness

Layered Defense

To protect the people, process, and technology phishing attack vectors, organizations deploy layers of information security defenses. Phishing-specific defenses generally fall into the two broad categories of filtering solutions and security awareness education.

Filtering

Every year there are stunning advancements in the effectiveness of traditional filtering and blocking solutions designed to prevent the delivery of untrustworthy electronic messages. Web-content filters can reduce the potential impact of phishing attacks by limiting the exposure to untrustworthy websites. Data Loss Prevention (DLP) solutions work to prevent the direct transmission of confidential documents.

Filtering is a critical layer of security controls. Nonetheless, almost everyone still receives those questionable communications that sneak through the filters to land in the trusted domain of the Inbox.

Attackers know that once a message reaches a user, there is a chance he will share sensitive data.

Education

The goal of security awareness education is to reduce the chances of unauthorized data disclosure by arming employees with the knowledge to recognize, repel, and report phishing attacks.

Training is a critical layer of protection that is much more difficult to objectively measure than automated controls.

Gain the Attacker Perspective

PhishLine®
Measured Security Awareness

Gain the Attacker Perspective

Filters and education never quite seem to be enough to keep people from directly or indirectly disclosing sensitive information to determined phishing scammers.

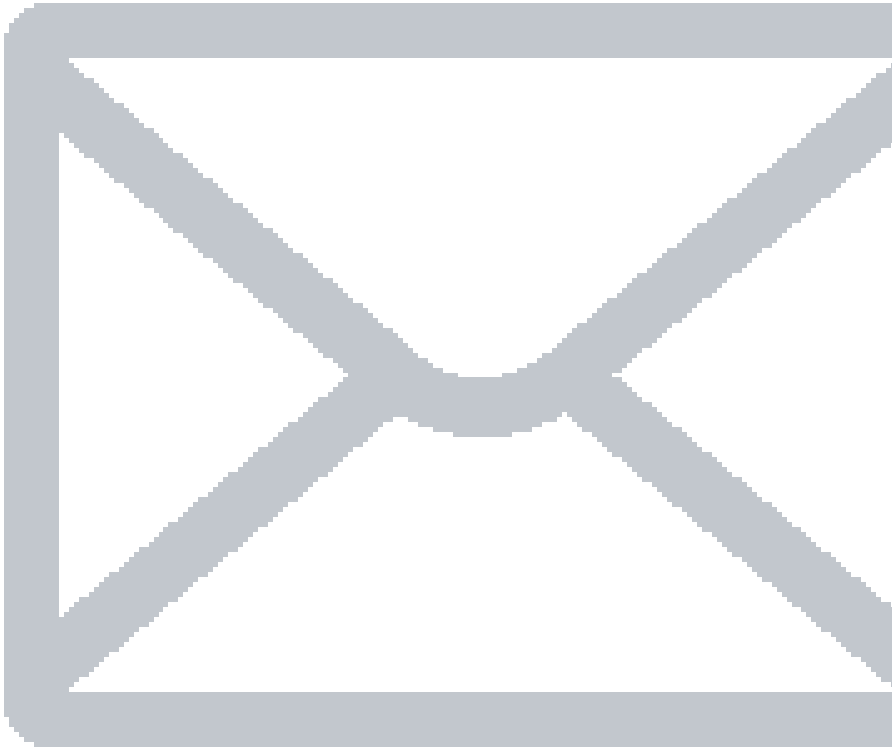
To effectively thwart an attack, it is necessary to know your opponent.

Attackers Persistently Test Your Defenses

In the technology arena, attackers often have an unfair advantage in understanding their prey because they can easily evaluate the latest commercial defenses in search of ways to foil the protection mechanisms. To be successful, all they need is one way to break through.

In the rare case of custom solutions or non-automated controls, an attacker may be able to simply do black-box testing with the persistent theme of “try, try again.”

To further complicate the issue, valid emails must be delivered while filtering out the bad messages. Although white-listing and similar techniques may work in certain environments, the vast majority of users require a method to receive messages from a wide variety of sources.



Perform Phishing Vulnerability Assessments

In the traditional technical vulnerability assessment world, organizations periodically perform advanced infiltration tests against production systems to gain insights into the attacker's viewpoint. The results of these authorized tests lead to more effective controls.

To help understand the effectiveness of anti-phishing controls, organizations must arm themselves with some of the advanced techniques used by phishing attackers to gain insights into weaknesses in their defense infrastructure.

Building on what was learned in the traditional vulnerability assessment practice, the testing solutions must provide actionable information and a reasonable margin of safety. Like the attackers, the techniques must be persistent, relevant, and bold.

PhishLine enables organizations to perform unlimited objective tests in an automated manner. The system's power provides deep insights into the people, processes, and technology that are most vulnerable while safely emulating attacker techniques.

Traditional Testing Approaches

There are several traditional approaches to test the vulnerability to phishing attacks.

1. **Do it yourself** – Open up a few disposable email accounts and create a landing page on a free web-hosting site. Send out a large batch of emails and gather the results. It is a manually intensive process that may inadvertently introduce additional security risks if users provide sensitive information.
2. **Hire a consultant to perform a "social engineering penetration test"** – Let the consultant do what you were going to do yourself. One-time results and scope limitations depend on the skill and tools provided by the specific consultant.
3. **Purchase a Security Awareness Training System** – Be sure it has a testing module. Determine if the system is designed to test the users' knowledge of the supplied awareness content or if was designed to simulate real-world multi-faceted phishing vulnerability tests.

Safe and Actionable Attack Simulations

PhishLine is designed to provide targeted information security awareness content and sophisticated phishing vulnerability assessments while using proprietary methods to limit the collection of actual confidential information.

The security awareness training module provides content, delivery, and testing mechanisms. It is fully integrated with the vulnerability assessment module.

Vulnerability assessments examine information shared by the browser to identify potential security holes. For example, when a user clicks on a link, the browser may reveal that it is a very old version with obsolete plugins. PhishLine then identifies specific potential vulnerabilities without performing dangerous exploitation tests.

From a technical perspective, the main difference between a vulnerability assessment and technical penetration testing is the payload. Technical penetration tests use malicious payloads to actually exploit vulnerabilities, compromise systems, and extract data.

	Security Awareness Training	Phishing Vulnerability Assessment	Technical Penetration Testing
PhishLine	Strong	Strong	Prevented*
Competitors	Strong	Weak	N/A
Open-Source	N/A	Weak	Strong

*Patent-pending technology allows for strong vulnerability assessment capability without actually performing penetration testing and putting critical information assets at-risk.

Table 1. Comparative Strengths of Training and Testing Solutions

Minimize Collection of Sensitive Information

The responsible way to perform a phishing vulnerability assessment is to only collect the least amount of information possible to provide metrics and direct remediation activities.

For example, passwords should not be collected or stored. The best practice is to only collect information that a password was entered.

For mobile device assessments, it is easy to configure the landing pages to collect location information. As PhishLine examines the GPS location information, it does not capture longitude, latitude, altitude, or speed for privacy reasons. It may be configured to collect the “accuracy reading” for non-repudiation purposes.

Fit the Organizational Culture

PhishLine®
Measured Security Awareness

Fit the Organizational Culture

Regardless of the specific method, it is critical to train, test, measure, and share in a manner that is consistent with the culture, philosophy, and work environment in the specific organization.

For some organizations, there are cultural or contractual barriers to any type of employee testing. Some even have restrictions on the types and methods of employee training.

Many organizations embrace the idea of safely testing the human firewall. It is viewed as a logical and important extension to traditional security vulnerability assessments.

Avoid Resentment

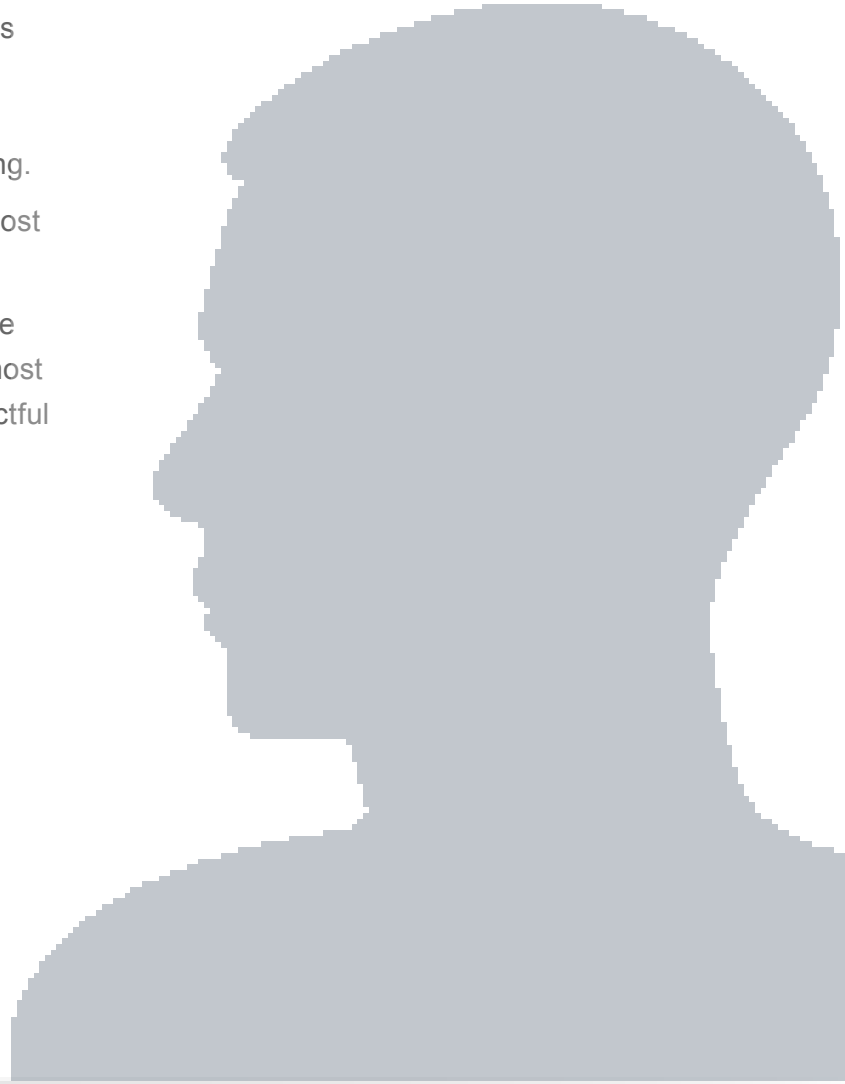
When done properly, training, testing, measuring, and sharing provides measurable improvements in the organization's security posture with respect to phishing attacks.

When done improperly, users may feel embarrassment and resentment.

PhishLine is not a trivial tool to simply "trick" employees. It is an enterprise ready, professional solution that can make a real difference in reducing risk exposure when used in a manner that is appropriate for the environment.

It is best used in concert with mature, relevant, and focused enterprise information security programs.

- **Individual Results** – It is imperative to plan how individually identifiable results may be shared before providing training or testing. There are almost no situations where internally publishing the list of the most susceptible individuals would be helpful in any way. The software can be configured to maximize anonymity while using individual test results to target specific security awareness follow-up training.
- **Share Group Metrics** – Publishing objective group-level metrics is one of the most powerful ways to help increase awareness and change behavior.
- **Provide Private Reinforcement** - Privately provide reinforcement targeted to the individual by using a learning method that is most appropriate for the user and most practical for the organization. Again, this may be done through anonymous or tactful analysis of testing results.



How Attackers Circumvent Spam Filters

PhishLine®
Measured Security Awareness

How Attackers Circumvent Spam Filters

There are several techniques to consider when acting like an attacker. Just like in the traditional vulnerability assessment testing world, these techniques are well-known by the bad guys. There is little risk of teaching them something new here.

Highly Permuted Campaigns

It used to be that a single message would be sent to many users. It would take a long time before the sender, IP Address, or message signature would be identified and blocked.

Today, the protection systems are getting much more sophisticated and blockable attributes are identified fairly quickly. Our recent experience shows that many enterprise filtering solutions will block a single new suspicious message in less than 150 emails if sent in bulk. (The amount of sensitive information typically disclosed by a subset of the 150 users can be an eye-opener.)

Attackers work around traditional filters by providing a high number of permuted variations of a message. For example, if you send out 50 variations of an email from 100 domains with 10 landing pages, that leads to 50x100x10 = 50,000 unique combinations.

Table 2 shows that it does not take much effort to get over one million permutations.

Illustration of Permutation Effects			
Email Messages Variations	Email Sender Account Variations	Landing Page Variations	Total Possible Permutations
1	1	1	1
10	10	10	1,000
25	25	25	15,625
200	200	25	1,000,000

Table 2. Illustration of Permutation Effects.

Of course, if a particular area is identified and blocked, such as the email sender account, it will greatly reduce the effective number of possible permutations. It is obvious that a very large number of variations in a particular area would increase the attack effectiveness. Given the indirect feedback loop of user interaction, it is quite possible to automatically identify which attributes are most effective.

Admittedly, this type of advanced analysis is not typically necessary. Simple variations tend to be effective when combined with other malicious techniques. PhishLine is a leader in implementing innovative highly-permuted message variations and advanced variation analysis.

Blitz vs. Low-and-Slow

The rate of message delivery is another important factor to circumvent automated filtering solutions.

One technique is to use an email blitz, where a very high number of emails are delivered in a short time period. While this is likely to be caught in a spam filter, usually a reasonable number are delivered and opened by users before the door closes. If sent at the right time of day, which is approaching any time in this 24x7 always-connected work-world, dozens if not hundreds of users will have the opportunity to interact with the email blitz.

Another technique is to go low-and-slow. The math is easy. Just send a few emails each day using the highly permuted technique above. It is amazing the number of emails that can be delivered before they are caught. Many low-and-slow permutations go undetected.

Consumer Trends Increase Risk

PhishLine®
Measured Security Awareness

Consumer Trends Increase Risk

There are several trends that are leading to increased risk to spear-phishing attacks.

Mobility

Intelligent mobile devices increase the susceptibility and impact of phishing attacks due to the small form factor, incredible connectivity, and location capabilities.

The limited screen size often reduces the ability to see all relevant information. For example, the “from” field may only show the sender name, not the actual email address. The result is that an email that appears on the screen to be from “Fred Jones” is really from “Fred Jones <thisisnotfredjones@spearphish.com>”.

Mobile devices often include multiple communication paths including email, text-messages, and social network accounts. These paths are highly integrated and become tempting targets in their own right with Virtual Private Network (VPN), Wireless Networking, and other access credentials.

Finally, the impact of attacking mobile devices may be increased as many are designed to share physical location information using Global Positioning System (GPS) or other methods.

Bring Your Own Device (BYOD)

When technology was relatively expensive, the global enterprises were masters of the technology domain with tight control on features, availability, and security.

The low price points and high-availability of advanced consumer solutions has greatly increased the number and types of devices that people are bringing to the enterprise.

This is not just about the device. Users are now engaging in **Bring Your Own Everything** such as Wireless Networking, Internet Access, Messaging Platforms, Storage, Backup, Security, and Integrated Business Applications. The latter goes beyond simple 'apps' and into the world of enterprise-grade personally-consumed cloud-based application platforms.

Sensitive information is more likely to be transmitted, processed, and stored beyond the traditional enterprise controlled environment. Furthermore, secure remote access through Virtual Private Networks and integrated messaging platforms may directly expose enterprise resources to non-enterprise devices.

Privacy and ownership issues of the BYOD trend often limit the ability for the enterprise to provide even basic solutions such as anti-virus, patch management, and message filtering solutions.

The result is that BYOD is exposing a whole new class of ripe targets for exploitation. Phishing techniques are an easy avenue for a determined attacker to compromise these devices.

Social Networking

An obvious compelling force driving the popularity of social networking is the desire to easily share information – which is the opposite of confidentiality and privacy.

While many social networks are non-business related, many organizations and professionals are leveraging these tools for sales, marketing, and recruitment efforts.

Attackers know that employees may respond to social engineering attacks that masquerade as valid invitations, notices, and other communications.

Security Awareness Training

PhishLine®
Measured Security Awareness

Security Awareness Training

There is no substitute for having an effective ‘human firewall’ where employees thwart unauthorized information access requests. In spite of the excellent training and educational materials available, it is typical to train employees but never test how well they resist the temptations of a compelling phishing message.

It is also an ongoing challenge to keep them motivated.

Content and Curriculum

There are many great sources for effective information security awareness training content. Organizations may want to leverage existing investments or they may want to provide fresh new materials.

Different people learn different ways. Some prefer computer-based training. Others learn better in a traditional instructor-led classroom. Still others retain knowledge best with hands-on interactive activities.

PhishLine provides messaging, targeted awareness, and questionnaire-based training modules. It can also be used to track and measure the effectiveness of other training methods unrelated to the system.

The challenge is to provide the most appropriate content to the most susceptible people.

Motivation

There is more to awareness than just training on the specific techniques. There must be an emphasis on how to keep people motivated and diligent.

In the years leading up to and following the development of PhishLine, we found the simplest and most effective motivational techniques for most enterprise environments are:

1. Let users know that they are going to be tested on a regular basis.
2. Share useful performance metrics. Use “competitive spirit” metrics where appropriate.
3. Show users what kind of information their browsers broadcast to every site visited.
4. Provide repetitive, targeted, reinforcement.

Measure Results

It is imperative to objectively test the results.

The traditional approach is to provide a quiz that reinforces the security awareness training content. Nothing new here, users must answer a high enough percent of the questions to pass.

The more important metrics are the results of simulated phishing campaigns. Each campaign uses the speed and variation tips discussed above combined with results-oriented message content and landing pages.

For example, if users have been trained to never enter a password on an http: website instead of an https:, the message content may contain a link to a login and password form on a simulated insecure site. Based on the percentage of people who enter a login and password on the site, an organization may direct additional security awareness efforts to address the specific shortcoming.

Target Your Methods and Take Action

Measuring results is only useful if it provides actionable data. It is imperative to use the metrics to drive remediation actions.

In an appropriate manner, users may be targeted with educational messages that anonymously escalate based on the previously measured susceptibility to prior attacks. For example, the first time a user enters a password on a simulated untrustworthy site, they receive a gentle reminder that reinforces the educational material. The second time, they may receive a more strict warning with a requirement to retake portions of the security awareness training. The third time may result in adding user-specific restrictions on the corporate content filter to mitigate the risk.

The important concept is that targeted, escalating action may be taken.

Should reinforcement directly follow a triggering event?

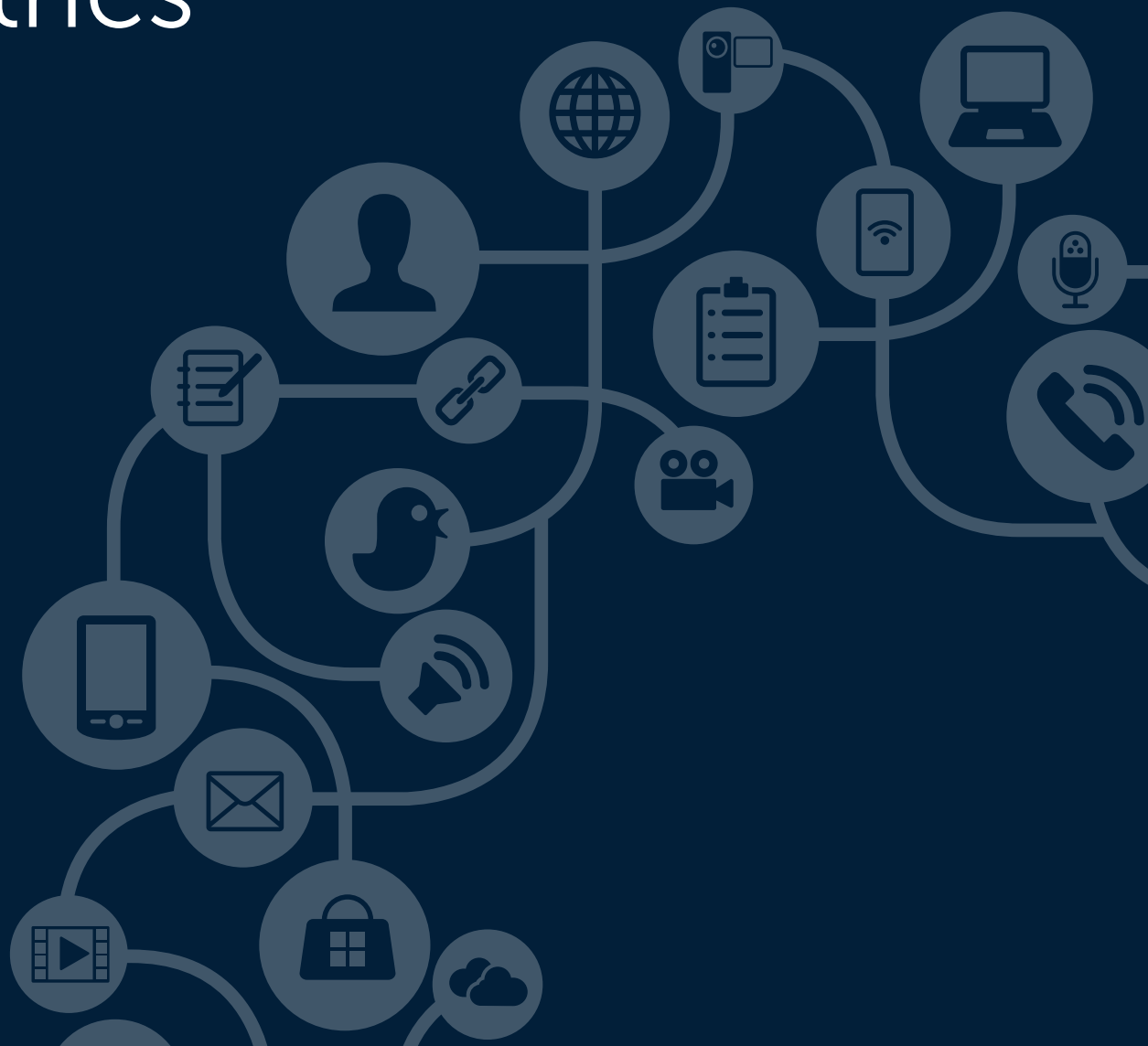
When users interact with untrustworthy messages, it does not feel much different than normal communications. In both scenarios, a user receives a message and can reply or click on a link.

On the one hand, many feel that as soon as the user clicks on a link they should receive relevant educational materials to reinforce what they did wrong at the time closest to the incorrect behavior. Numerous educational and training approaches reinforce the concept of immediate feedback.

On the other hand, is it reasonable to expect a user to be in an “optimal learning mood” immediately after they are informed that they were tricked? Or, can this cause resentment? Perhaps targeted educational reinforcement should occur at a controlled time and method.

Before testing users, the training approach should be in place. There is more than one right answer, and it often depends on what was communicated before the testing started.

Clear and Actionable Security Metrics



PhishLine®
Measured Security Awareness

Clear and Actionable Security Metrics

Many organizations spend money on security awareness and filtering solutions without providing objective, understandable, and actionable metrics.

PhishLine was designed to provide actionable metrics

PhishLine customers appreciate easy to understand **user behavior metrics** like the following samples**:**

- Last month, 61% of all employees proactively engaged with this particular suspicious email message.
- This quarter, the mock phishing campaigns collected evidence that 2,089 passwords were entered on this particular untrustworthy-looking web page. Most were from a certain division or country.
- 18% of all employees who received this request attempted to share a sensitive file.
- Users tend to be more susceptible on Mondays, less susceptible mid-week.

And for the technical metrics:

- 8% of all interactions were from personal iPads.
- 65% of those iPad interactions were on systems with insecure software versions installed.

Finally, metrics should relate to the actions taken.

- 320 people automatically received targeted remediation training.
- 20 people are scheduled for a special training workshop next month.

About the Author

PhishLine®
Measured Security Awareness

About the Author

Mark T. Chapman, CFE CISSP CISM CRISC

President & Founder, PhishLine

Mark is the president and founder of PhishLine and has spent the majority of his 20+ year career leading talented teams in the development of cutting-edge solutions in the areas of risk management, information security, and social engineering. Mark has extensive experience addressing security concerns for a wide variety of enterprise customers who keep him closely connected to the information security community and the challenges within.

PhishLine is the next generation solution for Measured Security Awareness. Designed as an enterprise level platform for testing, training, and measuring susceptibility to social engineering threats, PhishLine helps organizations progressively strengthen their user-level security posture.

Mark is a popular and engaging speaker that has been chosen to present on behalf of several professional associations, including ISACA, ISSA, and Infragard. Mark has also presented his research findings at conferences in the United States, Asia, and Europe.

Mark earned both a Bachelor's Degree in Computer Science and a Master's Degree in Computer Science in the area of Cryptography and Data Security from the University of Wisconsin-Milwaukee. His Information Security Certifications include: CFE, CISSP, IAM, CISM, and CRISC.

Mark resides with his wife of over 20 years, Cheri, in Muskego, Wisconsin.

About PhishLine

PhishLine®
Measured Security Awareness

About PhishLine

PhishLine was launched in 2011 to help Information Security Professionals meet and overcome the challenges associated with social engineering and phishing. PhishLine was met with instant praise and rapidly became the signature brand of Chapman Technology Group. Now a standalone company, PhishLine continues to receive widespread recognition throughout the information security community for bringing objectivity and actionable metrics to an area of information security that has needed them.

PhishLine has become the next generation solution for Measured Security Awareness. Designed as an enterprise level platform for testing, training, and measuring susceptibility to social engineering threats, PhishLine delivers vivid metrics and reporting capabilities that arm security teams with an unparalleled level of visibility and control. For more information visit www.phishline.com.

www.PhishLine.com

sales@phishline.com

262.546.1867

20800 Swenson Drive Suite 125, Waukesha WI 53186