Executive Summary

Phishing is defined by the Financial Services Technology Consortium (FSTC) as “a broadly launched social engineering attack in which an electronic identity is misrepresented in an attempt to trick individuals into revealing personal credentials that can be used fraudulently against them. In short, it’s online fraud to the highest degree.”

Although it’s been around for years, phishing is still one of the most common and effective online scams. The schemes are varied, typically involving some combination of spoofed email (spam), malicious software (malware), and fake websites to harvest personal information from unwitting consumers. The explosive rise of mobile devices, mobile applications, and social media networks has given phishers new vectors to exploit, along with access to volumes of personal data that can be used in more targeted attacks or spear phishing. The fact that phishing attacks are still so common highlights their efficacy and reinforces the need to implement comprehensive phishing and response plans to protect organizations.

Both large and small businesses are targets of this pervasive form of online fraud. PayPal, Apple, American Express, Amazon and Facebook are just some of the organizations that have consistently been victims of phishing attacks, along with thousands of their customers and users. In addition, financial firms and social media companies are top phishing targets. Kaspersky Labs reports that nearly 30 percent of all phishing attacks in 2013 targeted financial institutions, second only to social networking phishing attack campaigns.

The goal of any organization is to prevent or minimize the impact of phishing attacks. This can only be achieved by the development and implementation of a comprehensive phishing protection and response plan. In all cases, the plan’s success hinges on solid support and ongoing communication throughout the entire organization.
Phishing attacks continue to create concern with fraud prevention experts working to defend online brands from identity theft, monetary losses and erosion of consumer confidence. The Anti-Phishing Working Group (APWG) reports that an average of more than 500 unique brands are being targeted every month, with online payment processors leading the way in attack volumes. The number of unique phishing attacks detected by AWPG in Q1 of 2014 alone exceeded 125,000, the highest number seen in a single quarter since 2012. Phishing attacks can have a devastating impact on revenues, customer relationships, marketing efforts, and brand perception. Each attack can cost thousands to hundreds of thousands of dollars per attack in fraud-related losses and personnel time. Even worse, costs associated with the damage to brand image and consumer confidence can run in the millions of dollars.

Key objectives of an effective phishing protection and response plan should include:

- Identification of appropriate stakeholders and their responsibilities
- Ensuring compatibility with existing processes, including consideration for daily operational flow, size of organization, and availability of resources
- Creation of effective internal/external communications process
- Development of a solid phishing response escalation plan
- Minimization or avoidance of negative customer experiences
- Reduction of financial losses due to online fraud
- Proactive protection of corporate reputation
- Routinely educating employees about existing threats and social engineering tactics through cyber safety awareness training

Four Steps: Prevention, Detection, Response, and Recovery

An effective phishing protection plan should focus on four primary areas: Prevention, Detection, Response, and Recovery. High-level recommendations for each of the four areas are outlined in the following sections.
Phishing is first and foremost a human-driven problem. Therefore, phishers will attack trusted brands that provide the least resistance, enabling the highest return for their efforts. Your goal should be to make your organization extremely difficult for phishers to successfully mount an attack. Here are five ways to make it more difficult for phishers to attack your organization:

**Establish Ownership and Accountability**

All too often, an organization's first response to a phishing attack is reactionary. The attack and its consequences become an organizational "hot potato" with ambiguity surrounding what to do next. Before you’re attacked, it’s crucial to identify a central authority before you’re attacked with clear accountability for policy and action. It will streamline communications, which are critical in the throes of an attack. In addition, set up appropriate Emergency Response Teams with clearly defined roles and responsibilities. Also, create a Phishing Abuse Hotline or special inbox for customers and employees to report suspicious email messages.

**According to the annual RSA Fraud Report, phishing resulted in estimated losses of USD $5.9 billion in 2013.**
Educate Employees
The weakest link in an organization’s IT security plan is often its own employees. Using social engineering, malicious emails, spear phishing, and other tactics, criminals are often able to trick employees into disclosing private information or bringing malware inside an organization. In recent surveys, nearly half of all security, risk, and compliance officers have indicated that their own employees are a greater risk than hackers or hacktivists. Implement cyber safety awareness training that uses real life examples taken from news headlines, relevant research, and experience from open source threat intelligence. Training like this will enhance your employees’ knowledge of the types of threats and threat vectors that encompass today’s phishing attacks.

More than a million phishing attacks are launched every year, affecting hundreds of online brands in private, commercial and government sectors around the world.

Educate Customers
All customer communications should include clear messaging about phishing prevention. Create corporate policies for email content so that legitimate email cannot be confused with phishing. This includes emails, account statements, direct marketing materials, etc. Be very clear with customers about the steps they should take if they’ve fallen victim to phishing or identity theft. Finally, be sure that policies about phishing are prominently displayed on your organization’s primary website.

Develop Consistent Customer Email Practices
Use consistent email formats and develop standard practices for customer communications. This consistency “trains” customers on what to expect upon receiving your email communications. This will increase the likelihood that the customer will easily spot a fraudulent email.
Conduct a Thorough Audit and Inventory of Online Assets

This includes registered domain names, both live and parked, all legitimate company mobile apps, and all websites with their corresponding URL’s that are owned by or affiliated with your organization. Having a complete, organization-wide inventory of all registered domains allows for fast identification of a newly registered domain name that may be used as part of a phishing attack.

Criminal activity has expanded beyond web and into mobile applications, or apps. As mobile apps and marketplaces have grown, cyber criminals have quickly exploited them as new threat vectors for malware, phishing and other types of fraud.

Stay abreast of all emerging trends and technologies being deployed by phishers to commit fraud. Also, become familiar with professional groups and associations like the APWG. In addition, build an international network of contacts in the legal, governmental and ISP communities. These resources will help to identify the sources of phishing attacks and get websites shut down quickly. Many of these attacks originate outside of the US, so it’s crucial to be prepared with a global escalation matrix.
Detection: Speed Is Everything

Detection is central to any phishing protection and response plan, and the speed of detection is crucial to limiting the amount of losses caused by a phishing attack. The longer a phishing website is live, the more potential it has to cause damage. The steps of detection are shown in this graphic and employ a number of strategies for detecting phishing attacks from junk email (spam).

How You Can Detect Phishing

- Obtain junk email from honey pot accounts or employ a service provider who can do this for you.
- Use pre-sorted email feeds from Internet Service Providers (ISP’s) and anti-spam companies.
- Filter both internally received spam and externally provided email feeds for attacks.
- Search the Internet to identify any websites masquerading as your organization’s website.
- Continuously monitor the Internet for suspicious new domain name registrations and changes to existing registrations.
- Provide 24 x 7 coverage of your organization’s fraud hotline and abuse email inbox.

The best protection from phishing is vigilance. The APWG reports that typical phishing websites are live for an average of five days, with some staying live much longer. The sooner a phishing website can be detected, the sooner it can come down. Effective detection methods can reduce the average phishing website takedown time from days to hours.
Your organization’s response to a phishing attack will ultimately determine the extent of damage caused by the attack. The faster a website is brought down the less damage it can cause. How your organization handles the attack will directly impact the effectiveness of the phishing website takedown procedures. An effective response plan should include the following components:

- After a phishing website is detected and confirmed, immediately initiate website takedown procedures using your internal staff or outsourced service provider.
- Assess the size and scope of the phishing attack.
- Obtain information about the website and the ISP hosting the website.
- Contact the ISP to request the website be removed and escalate to the ISP’s local authorities as needed.
- Maintain contact with the ISP until the website is brought down and is no longer a threat to your organization.
- Contact the appropriate individuals based on your organization’s escalation procedures.
- Provide the URL of the detected phishing website(s) to ISP's and security companies. These companies use the URL’s to block and/or alert their subscription-based members from gaining access to the fraudulent websites.
- Notify the appropriate legal authorities to report the crime.
- Alert your customers. The best way is to post an alert directly on your websites with a brief description of the attack.
- Create a Phishing Website Summary Report after the website is successfully taken down. This report will provide important historical evidence for investigative purposes.
Recovery from a phishing attack is just as important as responding to the attack itself. In this phase, you need to focus on minimizing the impact of the attack. Here are suggested elements for an effective recovery plan:

- Once a phishing website is shut down, work to gather all forensic information as well as any compromised customer data.
- Continue monitoring the website for at least 10 days to ensure the website does not go live again.
- Have press releases drafted and company statements prepared to address any external inquiries from customer or the media regarding a phishing attack.
- Search the Internet, message boards, and chat rooms to locate and retrieve your customers’ stolen credit card and debit card numbers, login names and passwords, and other personal information compromised from the attack. The quick retrieval of this information reduces the overall cost of the phishing attack and significantly improves customer attrition due to fraud-related events.
- Conduct a post-mortem on the attack to identify areas for improvement.
Phishing is a problem that will be around for the foreseeable future. Phishing schemes continue to proliferate because they work, and they are increasingly becoming more sophisticated and better able to hide from detection.

It makes good business sense to take a hard look at your company’s readiness, ascertain your preparedness, and devise a solid, aggressive plan to combat the problem of phishing. Doing so is a win-win for the security professional, the customer, and the business as a whole.
While your network may be secure, do you have visibility beyond the perimeter? Security is no longer about what you can see. What you can’t see is where the true threats hide.

Cyveillance offers an easy-to-use platform that enables security professionals the ability to see beyond the perimeter. Our solutions identify cyber and physical threats and risks across the globe, allowing you to mitigate and eliminate them before they disrupt your business.

We go beyond data to provide the threat intelligence that you need to achieve your organization’s business goals. Contact us today to learn more and get a free trial.


A study by Verizon has shown that the targets of 85 percent attacks are small businesses with less than 1,000 employees. Verizon, “2012 Data Breach Investigations Report.” http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf

www.cyveillance.com/cyberthreatcenter
Cyveillance is the leading provider of cyber threat intelligence, enabling organizations to protect their information, infrastructure, and employees from physical and online threats found outside the network perimeter. Founded in 1997, Cyveillance delivers an intelligence-led approach to security through continuous, comprehensive monitoring of millions of online data sources, along with sophisticated technical and human analysis. The Cyveillance Cyber Threat Center, a cloud-based platform, combines web search, social media monitoring, underground channel information, and global intelligence with investigative tools and databases of threat actors, domain names and IP data, phishing activity, and malware. Cyveillance serves the Global 2000 and the majority of the Fortune 50 – as well as global leaders in finance, technology, and energy – along with data partners and resellers. For more information, visit www.cyveillance.com.

Cyveillance is a wholly-owned subsidiary of QinetiQ, a FTSE250 company which uses its domain knowledge to provide technical support and know-how to customers in the global aerospace, defense and security markets. For more information, visit www.qinetiq.com.