Four Steps to Effectively Protecting Your Organization from Phishing Attacks
Executive Summary ................................................................. 3

Four Focus Areas: Prevention, Detection, Response, and Recovery

Prevention: Make Your Organization A Tough Target ...................... 5
Detection: Speed Is Everything ...................................................... 7
Response: Communication Is Key .................................................... 8
Recovery: Have A Process In Place .................................................. 9

LookingGlass Solutions ............................................................... 10

LookingGlass Protected Site Seal ................................................. 10
Dynamic Threat Defense ............................................................. 10
Detection and Analysis Service .................................................... 10
Response and Take Down Service ................................................ 11
MRTI: Phishing URL Data Feed ................................................... 11
Cyber Safety Awareness Training ................................................. 11
Summary ................................................................................. 12
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. One of the reasons for its popularity amongst attackers is the relative ease of deployment with a very broad target base. 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 protection 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, Google and Facebook are just some of the organizations that have been victims of phishing attacks, along with thousands of their customers and users. The Anti-Phishing Working Group (APWG) reported that the Retail/Services sector made up more than 40 percent of all phishing attacks in the first quarter of 2016. Phishing has even been attributed to causing some of the largest data breaches, such as Anthem’s 2015 breach that compromised approximately 80 million customers’ personal information.

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 loses and erosion of consumer confidence. The APWG reported that the number of phishing attacks increased 250 percent in the first quarter of 2016. There were more phishing attacks during those three months than any other three-month span since 2004. In addition, the organization detected approximately 290,000 unique phishing attacks in Q1 2016. 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.

**Establish Ownership and Accountability**

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. Set up appropriate Emergency Response Teams with clearly defined roles and responsibilities. Create a Phishing Abuse Hotline or special inbox for customers and employees to report suspicious email messages.
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. Additionally, a 2016 experiment showed that more than 50 percent of email recipients still click links from unknown senders. Implement cyber safety awareness training that uses real life examples taken from news headlines, relevant research, and experience from open source threat intelligence.

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.

Develop Consistent Customer Email Practices
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. Use consistent email formats and develop standard practices for customer communications including account statements and direct marketing materials. 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 domain names allows for fast identification of a newly registered domain name that may be used as part of a phishing attack. 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 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 (ISPs) 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 average lifespan of a phishing website is 24 hours. 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 ISPs 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 ISPs and security companies. These companies use the URLs 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 customers 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 decreases customer attrition due to fraud-related events.
- Conduct a post-mortem on the attack to identify areas for improvement.
LookingGlass Protected Site Seal

The LookingGlass Protected Site Seal is a trust mark displayed on the websites of organizations that utilize LookingGlass Anti-Phishing solutions. The seal is an indication that an organization is serious about protecting customers and employees from phishing attacks. By implementing the LookingGlass Protected Site Seal on your website, we will be alerted when someone tries to copy your website for malicious purposes. The seal also discourages potential attackers from targeting your organization for phishing activities. For more details, please refer to Protected Site Seal.

Dynamic Threat Defense

Once a phishing URL is identified, customers can take preventive action to completely block employees from reaching the URL. The LookingGlass Dynamic Threat Defense (DTD) solution stops phishing attacks by combining the LookingGlass threat intelligence management platform ScoutVision and threat mitigation platform DNS Defender. For more details, please refer to Dynamic Threat Defense.

Detection and Analysis Service

LookingGlass Detection and Analysis Service protects your business from early stages of a phishing attack, including pharming and malware. LookingGlass will only alert you to authentic and verified phishing attacks, eliminating the risk of false positives and unwarranted customer analysis. For more details, please refer to Detection and Analysis Service.
Response and Take Down Service
The LookingGlass Response and Take Down Service is closely integrated with our Detection and Analysis Service. Once a phishing URL is detected, the LookingGlass Response and Takedown Service works with ISPs and local and international law enforcement authorities to takedown the malicious URL. Our analysts offer support in 200+ international languages and have successfully conducted takedowns in 140+ countries. For more details, please refer to Response and Take Down Services.

MRTI: Phishing URL Data Feed
LookingGlass Machine Readable Threat Intelligence provides a wide range of threat feeds to help correlate internal events with external threat activities. We discover thousands of phishing attacks across hundreds of companies and websites. This global phishing data provides valuable insights about the bigger picture on phishing activities. The data we collect is part of our phishing detection service as well as a data feed. For more details, please refer to Phishing URL Data Feed.

Cyber Safety Awareness Training
LookingGlass Cyber Safety Awareness Training helps educate employees to make the organization a tough target for possible phishing attacks. It is delivered by experts in cyber security and can be integrated into existing learning management systems. The training has three modules:
1. Data Loss Through People
2. Data Loss Through Machines
3. Advanced Attacks
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.
LookingGlass Cyber Solutions delivers comprehensive threat intelligence driven security through a scalable solution portfolio of machine readable threat intelligence (MRTI), a threat intelligence management platform with 100+ data sources transformed into global Internet and threat intelligence, network-based threat mitigation, and threat intelligence services.

By addressing risks across structured Indicators of Compromise (IoCs), unstructured and open source data (OSINT), and internal network telemetry, customers gain unprecedented understanding into threats that may impact their business including cyber, physical assets, and third party partners.

Prioritized, relevant and timely insights enable customers to operationalize threat intelligence in an effective and efficient way throughout the threat lifecycle.