Phishing in Perspective: It Only Takes One

Recent events have shown that phishing attacks are widespread. An estimated eight million phishing emails are opened by users every day. Of those emails, 10 percent lure someone into clicking on a link.

Technology provides great frontline protection against the unruly number of suspicious emails received by corporate networks daily. But, attackers are constantly devising methods to circumvent technical controls, making it virtually impossible for any technology to be 100 percent effective. No matter how quickly technology vendors react, there’s always a new attack vector on the horizon.

The fact is that somehow, some way, one or more phishing emails will reach your trusted network – a vast ecosystem that includes employees, but also freelancers, contractors, suppliers, affiliated third parties, and anyone else with access to your systems. They should all be educated, aware and engaged in preventing phishing attacks. In addition, your organization must proactively plan to mitigate phishing risk.

Highlights:

Back in 2011, many predicted the demise of phishing with the takedown of the infamous Rustock botnet. However, 2013 proved to be one of the most active years on record for phishing attacks as the dismantling of the Blackhole Exploit Kit caused a resurgence in old-school delivery and social engineering techniques. Email-borne attacks continue to run rampant often leaving business exposed to malware, data breaches, and advanced persistent threats (APTs). Worse yet, increased sophistication and advances make modern phishing attacks more of a threat than ever. Optiv helps protect organizations from phishing attacks by leveraging a multi-faceted approach to enhance security.
Phishing at a Glance
The Threat: Phishing Techniques

SPAM:
Opportunistic email for ads.

Phishing:
Opportunistic spam with malicious intent.

Spear-Phishing:
Targeted emails where personal information was gathered and used to make the email "credible".

Clone-Phishing:
Content and recipient addresses from a previously delivered legitimate email are used to create an almost identical or cloned email.

Whaling:
Focused phishing emails against senior executives of a company.

Lishing:
Using LinkedIn to send phishing or spear-phishing messages.

Smishing:
Using SMS messages to send phishing or spear-phishing messages.

Preventing attacks and protecting data and information assets is a shared responsibility across your organization. However, while every member of your staff has a role to play in the larger security picture, the security staff will always bear the blame for vulnerabilities, weaknesses and breaches. Executives and employees expect they should be able to open any attachment or click on any link, without risk of compromising the company—and be savvy enough to avoid common traps that put the organization at risk. Organizations have an obligation to limit exposure through the use of strong technical controls, innovative awareness programs, and a commitment to continuously evaluate and sharpen their security efforts. So, how do you get there?

The Optiv Approach

The Optiv approach delivers a comprehensive methodology that covers the spectrum of defenses used to prevent phishing. By addressing the problem holistically, through a combination of people, process and technology, you can effectively reduce the chance that users will open the door to risk and prevent these attacks from doing significant damage to your organization.

In response to the persistent threat from phishing attempts, we recommend that organizations concentrate on the “Three Es” of email security—enhanced technology, employee focus and enterprise visibility.

The 3 Es of Email Security

- Enhanced Technology
- Employee Focus
- Enterprise Visibility

Enhanced Technology—Take a page directly from the hacker handbook and consistently innovate your approach to security. Attacks change constantly. Fortunately, security experts can be just as persistent and creative in how they prevent attacks. Explore new technologies, understand how threats are evolving and be relentlessly curious about how you can respond.

Limiting delivery of spam to users helps effectively reduce your attack surface. Recent innovations in the space include:

- Sandboxing inbound email URLs and attachments
- URL wrapping for on-click analysis
- Leverage cloud and hybrid solutions for protections and agility
Costs of a Phishing Attack

The costs of a phishing attack can be challenging to quantify. Industry estimates put annuals costs to U.S. businesses at around $5 billion. Here’s a way to think about the costs of phishing and related fraud at an institutional level:

<table>
<thead>
<tr>
<th>Hard Costs</th>
<th>Soft Costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Risk and expense of fraud</td>
<td>• Reputation and brand damage</td>
</tr>
<tr>
<td>• Increased compliance burdens and/or fines</td>
<td>• Customer satisfaction</td>
</tr>
<tr>
<td>• Post-incident remediation</td>
<td>• Loss of business</td>
</tr>
<tr>
<td>• Support calls and IT time and effort</td>
<td></td>
</tr>
</tbody>
</table>

Enterprise Visibility—Organizations that may fall prey to phishing attacks can take steps to mitigate risk and limit impact. While the primary vulnerability exploited at the start of an attack is people, all sorts of factors can intensify such an attack. Improperly configured hardware, poor access controls and improperly stored or unencrypted data can all contribute to greater risk. Understanding and correcting your vulnerabilities is critical. As part of your comprehensive approach to security, map out your vulnerabilities, regularly conduct a gap analysis, and aggressively test your systems. Besides testing, enable monitoring and incident response capabilities within your organization. Lastly, operationalize data from attacks to your systems. Use the data from attacks and incidents that were prevented to provide insight into the return on your security investment by measuring impact and results.

The Optiv Advantage

Optiv combines extensive expertise and advanced research with real-world experience, enabling us to provide unique insight into evolving security threats and trends. We work with more than half of the Fortune 100, and our consultants execute more than 5,000 consulting projects per year ranging from malware emergency response to performing groundbreaking research for the federal government. Optiv works with organizations to prevent attacks that try to penetrate and steal valuable data.

Optiv has helped thousands of organizations evaluate their defenses, conduct social engineering and phishing vulnerability assessments and test their systems against simulated adversarial attack scenarios. For more information about how to address challenges in your environment or to learn about new and emerging threats, contact us today at 800.574.0896 or via email at info@optiv.com. A complete listing of our services is available at www.optiv.com.
1. According to some estimates the Rustock botnet, which operated from 2006 until 2011, was responsible for as much as 40 percent of spam traffic at the time. The network was capable of distributing up to 25,000 spam emails per hour from a network of infected PCs. Source: Real Viagra sales power global spam flood by John Dunn, Techworld. Published: 15:44, 13 July 2009, http://news.techworld.com/security/119086/real-viagra-sales-power-global-spam-flood/


4. Protect Sensitive Sites from Phishing Attacks Using Features Extractable from Inaccessible Phishing URLs, by Weibo Chu, Bin B. Zhu, Feng Xue, Xiaohong Guan, Zhongmin Cai, published by: MOE KLINNS Lab, Xi’an Jiaotong University, Xi’an, China, Microsoft Research Asia, Beijing, China, Center for Intelligent and Networked System and NLIST Lab, Tsinghua University, Beijing, China, 2012, http://research.microsoft.com/pubs/193315/Phishing_Detection_v1.4.0.pdf

