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.[3] 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.[1] However, 2013 proved to be one of the most active years on record for phishing attacks[2] 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.

The Impact:

A Microsoft research paper from 2014 categorizes phishing as the third cyber-security threat globally and the first cyber-security threat in China.[4]

In 2012, RSA estimated global losses from phishing at $1.5 billion.[5] In subsequent years, losses have been estimated at $5 billion or higher.

The average cost per compromised record in the United States is $195[6] plus litigation expense from civil suits—that figure exceeds $200 in EU states like Germany.

The Target breach which affected 98M people started with a phishing attack at a third-party.[7]

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

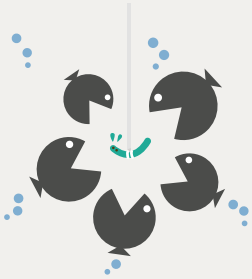
- Enhanced Technology
- Employee Focus
- Enterprise Visibility

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

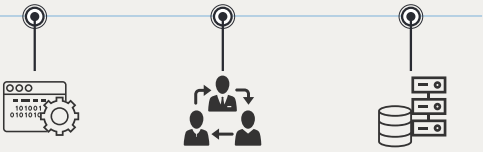
Costs of a Phishing Attack



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:

Hard Costs	Soft Costs
• Risk and expense of fraud	• Reputation and brand damage
• Increased compliance burdens and/or fines	• Customer satisfaction
• Post-incident remediation	• Loss of business
• Support calls and IT time and effort	

Optiv Solution Approaches



Testing

- Testing your current defenses and controls for efficacy and vulnerabilities
- Social engineering testing to determine susceptibility to targeted attacks

Training

- Just in time training
- User Awareness Education

Technology

- Network advanced threat detection tools
- Email and web gateway solutions

Employee Focus—Strong policies, employee incentives like a "Catch of the Day" email bounty program, and just-in time warnings delivered to the employee are foundational to any effort to address phishing. Regular training and awareness, when reinforced with technological controls, is essential for any phishing program. Education of your employees reduces your attack surface. It also improves response time, escalates the events efficiently, and can increase organizational agility when responding to an event. Education and awareness alone will not solve the problem but they are an essential part of an attack surface reduction effort and solution.

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/*

2. Phishing Attack Trends Report - 4Q2013, by Anti-Phishing Working Group, released Apr 27, 2014, Anti-Phishing Working Group, http://docs.apwg.org/reports/apwg_trends_report_q4_2013.pdf

3. Phishing Emails: The Scary Odds Of Success, by Rickard Darell, Bit Rebels, accessed June 11, 2013, http://www.bitrebels.com/technology/phishing-emails-statistics-infographic/

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

5. 2012 Global Losses from Phishing Estimated At $1.5 Bn, By Biztech2.com Staff, Published: BIZTECH Feb 20, 2013, http://www.firstbiz.com/biztech/2012-global-losses-from-phishing-estimated-at-1-5-bn-16850.html

6. 2014 Cost of Data Breach Study: Global Analysis, Benchmark research sponsored by IBM, Independently conducted by Ponemon Institute LLC, May 2014, http://public.dhe.ibm.com/common/ssi/ecm/en/sel03027usen/SEL03027USEN.PDF

7. Three New Details from Target's Credit Card Breach, By Ben Elgin, Published: March 26, 2014, Bloomberg BusinessWeek, http://www.businessweek.com/articles/2014-03-26/three-new-details-from-targets-credit-card-breach

OPTIV

1125 17th Street, Suite 1700
Denver, CO 80202
800.574.0896
www.optiv.com

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.

11.15 | F1