THE THREE Es OF MODERN EMAIL SECURITY FOR PHISHING

AN OPTIV VIEWPOINT

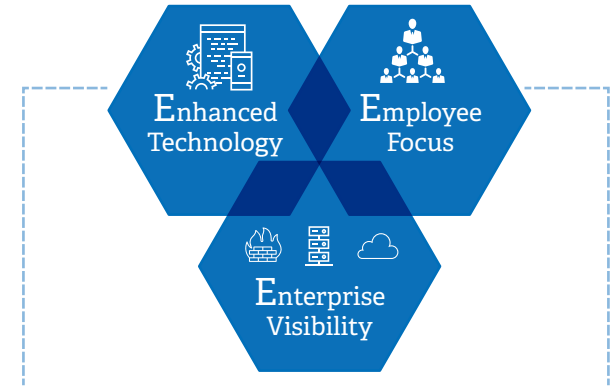
James Robinson, Director, Risk and Threat Management

Attempting to keep up with the ever-changing world of cyber security threats can be daunting. When you have an entire organization of hundreds or even thousands of employees – as well as a vast ecosystem of freelancers, contractors, suppliers, affiliated third parties, among others – who could unintentionally let an attacker into your environment, the problem becomes even more challenging.

Each day, more than a billion emails are sent containing malicious links and attachments, tempting users to take the bait and effectively launch an attack on your organization. Phishing emails are nothing new, but according to the Anti-Phishing Working Group, 2013 was one of the most active years for phishing. Because attackers are disguising and delivering these emails in more sophisticated ways than ever, most users aren't able to recognize a phishing attempt and many companies lack an effective strategy to address the issue.

Waiting until an attack occurs is not a good option. Consider using a three-pronged approach that combines in-depth defense, reduced attack surface and incident response plans. These three options make up our three Es of modern email security for phishing: enhanced technology, employee focus and enterprise visibility. By using this recipe, you can help prevent the financial fallout and loss of sensitive information for your organization.

The Three Es of Modern Email Security



Enhanced Technology

- Attachment Sandboxing
- URL Sandboxing
- URL Wrapping for On-Click Analysis
- Hybrid Delivery via Cloud/On-Premise

Enterprise Visibility

- Know Your Entry Points
- Enable Incident Response Capabilities
- Operationalize Data from Attacks

Employee Focus

- General Education and User Awareness
- Incentive Programs
- Continuous Testing

OPTIV

Enhanced Technology

The first of our three Es is Enhanced technology. This methodology offers improved protection and works to limit the delivery of phishing emails to users within your organization to reduce your attack surface. Most organizations I work with are trying to use spam filters as the primary means to block email phishing attacks. But they are only effective when an email is sent from a questionable source, and many times in spear-phishing the email is coming from a reputable source and bypasses the spam filter. New email security technologies are utilizing innovative features, designed to limit the delivery of phishing emails to users, and leverage concepts from Forrester's "zero trust model."

Attachment Sandboxing

New technologies are able to determine if an inbound email contains a malicious attachment by using a sandbox to open the file. This allows the file to be tested in a separate environment to ensure that it doesn't contain a virus or malware, without causing harm to the host computer.

URL Sandboxing

If there are any links in an inbound email, the technology is able to follow the link (in a sandbox) to determine if the destination is malicious. It is able to detect hidden iFrames and other elements that can direct the user to an environment containing an exploit or malware.

URL Wrapping for On-Click Analysis

Another tactic email security technologies use is changing and redirecting the URL. If a URL appears suspicious, it rewrites the URL and will do an analysis if and when a user clicks the link.

Hybrid Delivery via Cloud/On-Premise

An email is first delivered to a cloud environment, where the technology is able to examine it before it is delivered to an on-premise set of servers or appliances, after it has been deemed "safe." This allows you to keep the malware and the malicious emails off your environment entirely. The hybrid approach also allows URL wrapping to work from anywhere, on or off of your network.

Make it part of your job to explore new technologies, understand how threats are evolving, and innovate your approach to security.

Employee Focus

Following enhanced technology is our second E component, Employee focus. It is important that your employees are educated, aware and engaged in preventing a phishing attack. Relying on enhanced technology alone will never make you 100% successful in blocking phishing emails. Individuals need to know how to identify and react appropriately to a phishing email when they are targeted. The more people you have defending your environment, the better chance you can thwart an attack.

General Education and User Awareness

On-click education awareness is a great tactic to employ. Here's how it works: your organization sends a fake phishing email to its employees, and if they take the bait (e.g. click a link, download a file, enter information, etc.) they receive just-in-time education. Think about it the same way you would teach young children – when they misbehave, you can't punish them a few days later; you have to discipline them at that time so they understand what they did wrong. I'm not saying employees are children, but in our busy lives we all make mistakes, and the same principal applies. If an employee clicks on a malicious link, education should be delivered right away, so they can take the time to learn from the mistake, and then get on with their job. I have found this approach is much more effective than bringing employees into a room for an hour, telling them that they should worry about phishing, and providing information about some things they should do. In this second instance, the message doesn't resonate because it isn't top of mind. In fact, most of the time the employees glaze over the presentation and are more focused on the free coffee and doughnuts.

When you catch employees in the act, it tends to make a greater impact and stick with them, curbing the behavior in the future.

Incentive Programs

Creating programs that incentivize your employees can be a fun and effective way to get them involved in securing your organization's environment. They turn every employee into security personnel, and provide an avenue to escalate events for incident response.

"Catch of the Day" is an email bounty program where employees are encouraged to send any suspicious emails they receive to the IT security response team. The emails are then analyzed by the team and every month, the best one from across the organization is chosen. The winning employee is recognized and rewarded for their efforts in identifying the phishing attack. The prize can be something as simple as a $100 gift card – a small investment for your organization, but enough to get employees excited and motivated to participate.

Continuous Testing

Once you have put training and educational programs in place, it is important to test their level of success on an ongoing basis. You should send out different types of phishing emails to your employees and capture the results of these "tests." The aggregated results can help you understand the effectiveness of the programs you have in place and make any necessary changes to improve them. If you notice that people are more susceptible to download a file versus enter sensitive information in a form, you can use that data to tailor your education efforts.

Enterprise Visibility

Our last E in this three-pronged approach is Enterprise visibility. While the primary vulnerability exploited in a phishing attack is people, all sorts of factors within the enterprise can contribute to greater risk. Understanding and correcting your vulnerabilities is critical.

Know Your Entry Points

It is important to map out your vulnerabilities, regularly conduct a gap analysis, and aggressively test your systems to understand the entry points attackers can exploit. These entry points are constantly changing and evolving. For example, I was working with a company that merged with another organization that turned out to be wide open, without many security controls in place. This became a new entry point that wasn't being monitored, and the new, combined organization was hit with a phishing attack.

Enable Incident Response Capabilities

When a phishing attack is identified, it is critical that your organization has a process in place for proper notification and issue handling. Incident response plans should be mapped out for different attacks – from employee reports, to executive and public notification. You cannot wait until an attack has occurred, you must be ahead of the game with a plan. Being prepared makes a huge difference in how an attack impacts your organization.

Operationalize Data from Attacks

Every failed and successful attack should serve as a learning experience to your organization, and provide useful metrics and statistics. Use the data from attacks and incidents that were prevented to deliver insight into the return on your security investment by measuring impact and results. Use the data from successful attacks to understand the changes you need to make and how to prevent the exploit in the future.

Can you be sure your employee won't take the phishing bait and click on a link, successfully installing malware on their laptop and infecting your network?

Conclusion

There's a chance a phishing email is sitting in one of your employee's inbox right now. Can you be sure they won't take the bait and click on a link, successfully installing malware on their laptop and infecting your network? This may be a scary thought, but by using the three Es of modern email security to address phishing, you can effectively reduce the chance that a user will make that mistake.

Starting with a focus on technologies from attachment sandboxing to URL wrapping for on-click analysis, you can do more than simply hope phishing email gets caught in a spam folder. On the off chance that an email slips through your protections, people are your second line of defense. Educate your employees and others in your ecosystem about the risks, and provide on-click awareness to more effectively change behaviors. Put incentive programs into place to increase the chance of employees taking a productive part in securing your environment. Finally, knowing your environment top-to-bottom and understanding your entry points is vital to email security. If a phishing attack occurs, and the odds are that at some point it will, you must have an incident response plan in place. Gather data from both failed and successful phishing attacks to understand why they did or did not happen, and what you can do to improve your security posture. By understanding and putting these three Es of email security to work, you can help prevent your employees from opening the door to risk and prevent these attacks from doing significant damage to your organization.

James Robinson
Director, Risk and Threat Management

James Robinson is a seasoned professional with nearly 15 years of experience in security engineering, architecture and strategy. As director of risk and threat management in the Office of the CISO at Optiv, Robinson uses real world experiences to help enterprise-level organizations to solve their security and related business issues. He also develops and delivers a comprehensive suite of strategic services and solutions that help CXO executives change their security strategies through innovation. He ensures security executive success while aligning to business goals, bringing value to the community. Prior to his previous role at Accuvant, Robinson was the security architecture and strategy officer for Websense. In that role, he was accountable for internal security strategy development, innovation and implementation. He has held positions of increasing responsibilities with other Fortune 500 companies such as Anheuser-Busch and State Farm insurance where he ran one of the most successful penetration testing engagements in the company's history.

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.

10.15 | F1