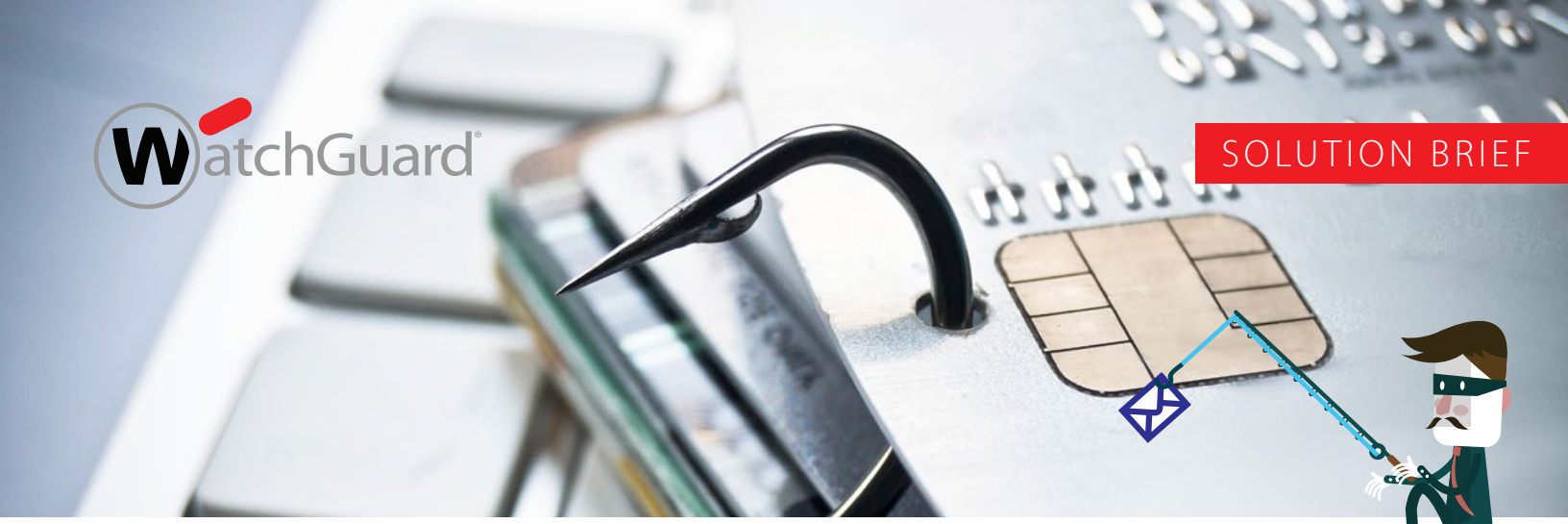

SOLUTION BRIEF

Don't Get Caught on the Hackers Line:

Protect Your Business from Phishing Attacks with WatchGuard

Introduction

Phishing attacks continue to be a top concern for small businesses and midsize enterprise organizations. In fact, 83% of businesses report being a victim of a phish attack in the last year alone.[1] This is not particularly surprising, considering that these attacks are straightforward to execute and particularly profitable for those who succeed.

But there is good news for IT admins – with a little phishing education and a layered defense, it is possible to protect your organization from a phishing attack.

What Is phishing?

The most common type of phishing attack is when a criminal sends an email pretending to be someone or something they are not, to extract sensitive data from the targets. They often use tactics to elicit fear, pique curiosity, or drive a sense of urgency to compel the target to open an attachment or click a malicious link.

What can be even more effective for a hacker, is to wage a highly-targeted spear-phishing attack – emails that include specific information pertaining to the target. Attackers will often research their target on social media channels like LinkedIn and Facebook to build a profile of their intended victim that will help them craft a tailored message that improves their chances for success.

Defending Against Phishing Attacks

The most successful anti-phishing programs have four components: Protection, Education, Evaluation, and Reporting. These four steps work together to use your staff as a human shield, enabled by technology.

Protecting against phishing requires a layered approach to security that aims to keep users safe on the Internet. Keys to this layered approach include:

- Monitoring and blocking malicious outbound DNS requests to ensure employees are not able to reach bad sites through suspicious links or communicate via command and control channels.
- Scanning tools to ensure that malicious files don't make it through the network, and endpoint security that can detect and kill malware.
- Cloud sandboxing solutions that allow you to detonate suspicious files in an emulated virtual environment that mimics an authentic endpoint to uncover malicious intent.
- Multi-factor authentication to guard against fraud, impersonation, and credential theft.

It's also critical to provide regular phishing education to your employees, along with evaluating their click rates. There are a variety of free and paid options available for training, including computer-based awareness training sessions, phishing email simulation exercises, and

[1] https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

even just sharing phishing education videos and posters with staff. Organizations with well-trained employees that pass regular and accurately reported-on phishing tests could have as low as a 5% susceptibility rate.[2]

As part of the education, it's important to let your staff know where they should forward emails they think are suspicious. Often, this is either forwarding the suspect email to the help desk or IT. These phishes are gold when it comes to understanding the how and who of an attack. By collecting and paying attention to phishes, you can sense trends in how your organization is being attacked (Office 365 phishes, Fake Invoices, etc.) and who (Sales, R&D, HR) are the targets. The attacker is effectively tipping their hand and we can use this to focus our security program and provide better protection.

Phishing Protection from WatchGuard

Every organization has their share of happy clickers. And even if only a small percentage of your employees are likely to click on an unsafe link or download an infected attachment, you need to have the right security services in place. With WatchGuard, you're able to protect end users from an attack, while reinforcing phishing education in the moment.

Protecting Against the Happy Clicker

DNS is the backbone of the Internet, functioning as the de facto phone book that translates domain names into IP addresses. DNS allows the average user to navigate to google.com instead of entering a numerical IP address. DNS is almost always the first step in the process of connecting to the Internet and is used by nearly every device that needs a connection. It is also one of the tools of choice for hackers who fool users and redirect traffic to malicious servers by spoofing the DNS record of legitimate sites.

As a first line of defense, inspecting each DNS request to determine which is malicious and which is legitimate can prevent a user's risky click from turning into a major security incident. With WatchGuard's Cloud-based DNS-level security solutions, malicious DNS requests are automatically detected and blocked based on the latest threat intelligence.

WatchGuard Offers Two Flavors of DNS-level Protection:

- DNSWatch – Included with the Total Security Suite, DNSWatch provides protection for all users connected to your network and behind a WatchGuard Firebox.
- DNSWatchGO – Provides lightweight, always-on protection against phishing and malware, for users on the go.

Both offerings provide immediate security awareness training to users when they encounter a phish, reinforcing the security education you've already provided. Reminding your employees about their training as they've just clicked on a link or attachment is the most effective way to prevent this from happening again. Coupled with this training is a message from you, maybe asking them to call you or forward the email the user just clicked on.

Defending Against Fraud, Impersonation, and Credential Theft

Lost credentials prove to be one of the most effective ways for hackers to breach a network, allowing an attacker to have full access to corporate resources and even impersonate their victim to cause further harm. Given the prevalence of credential stealing malware and poor password habits that are all too common, relying on usernames and passwords alone is no longer an option.

WatchGuard AuthPoint allows you to control access to assets, accounts, and information using multi-factor authentication. AuthPoint adds an additional layer of attestation compared to simple username and password authentication. Logins with AuthPoint are facilitated using a mobile phone and require something you know (password), you have (mobile phone), and you are (fingerprint, biometrics) to authenticate a user. Delivered from the Cloud, AuthPoint makes it possible to eliminate the risk of weak or stolen passwords.

[2] https://siliconangle.com/blog/2017/11/30/phishing-attacks-cost-1-6m-average-enterprises-successfully-fighting-back/

Killing Credential-Stealing Malware

Credential-stealing malware, or malware that seeks to steal usernames and passwords, is common, and consistently among the top 10 malware threats the average business encounters.[3] Detecting and killing these and other malware threats simply isn't possible with signature-based antivirus alone.

WatchGuard Offers Several Security Solutions to Detect and Kill Malware:

- **Gateway AntiVirus and IntelligentAV** - When a user is connected via your network, WatchGuard Gateway AntiVirus and AI-powered IntelligentAV scan files and traffic flowing through your Firebox to identify malware and riskware. If a threat is identified, the connection is blocked or the file is stripped. This protects employees from malicious attachments included in a phishing attack from ever reaching the end user waiting for a chance to click.
- **APT Blocker** - For evasive and zero day threats reaching your network, like those seen in highly targeted spear-phishing attacks, WatchGuard APT Blocker provides an additional layer of protection. APT Blocker executes the file in a Cloud sandbox and analyzes its threat potential. Malicious files are quarantined and system administrators are alerted of the threat.
- **ThreatSync** - ThreatSync is WatchGuard's Cloud-based correlation and threat-scoring engine, improving detection and response across the environment from the network to the endpoint. If malware is detected, ThreatSync will move to contain the host, quarantine the file, kill associated processes, and delete registry key persistence.

[3] https://www.watchguard.com/wgrd-about/press-releases/new-security-research-reveals-password-inadequacy-top-threat-need-mfa

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by nearly 10,000 security resellers and service providers to protect more than 80,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for midmarket businesses and distributed enterprises. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

For additional information, promotions and updates, follow WatchGuard on Twitter @WatchGuard, on Facebook, or on the LinkedIn Company page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at www.secplicity.org.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com