Don't Get Caught on a Hacker's Line

Protecting Your Business from Phishing Attacks with WatchGuard Total Security Suite

Introduction

Phishing attacks continue to be a top concern for small businesses and midsize enterprise organizations. In fact, 76% of businesses report being a victim of a phish attack in the last year alone.[1] Which 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?

A 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 common tactics such as eliciting fear, curiosity or a sense of urgency to entice the target to open an attachment or click a malicious link.

What can be even more effective for a hacker, is to wage a spearphishing attack – emails that include specific information pertaining to the target. Attackers will often research their target on social media channels like LinkedIn or even your corporate website to craft the perfect email guaranteed to make them click.

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.

The first pillar in any anti-phishing program is to provide protection by putting a barrier in between your happy clickers and the attackers by:

- Monitoring and blocking access to malicious outbound DNS requests that ensure employees are not able to reach bad sites through suspicious links.
- Scanning tools that monitor file behaviors to ensure that malicious files don't make it through the network.
- Using cloud sandboxing solutions that allow you to detonate suspicious files in a virtual environment to determine whether they are malicious. If the file is determined to be malicious, it will be quarantined, protecting the network from the attack.

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 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.

1 https://info.wombatsecurity.com/state-of-the-phish

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

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 Total Security Suite, you're able to protect end users from an attack, while reinforcing phishing education in the moment.

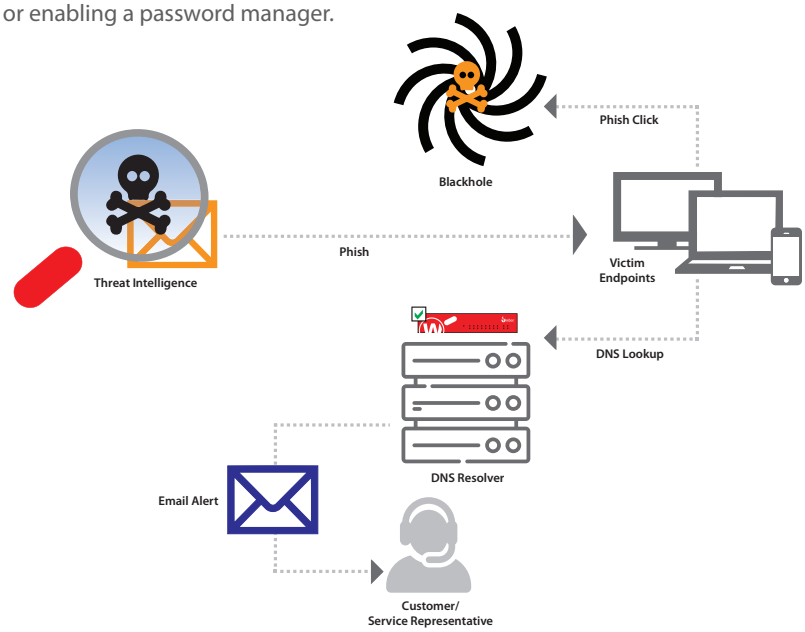
WatchGuard Gateway AntiVirus scans files and traffic flowing through the Firebox to identify known malware and riskware.If a threat is identified based on signature matching, the connection is blocked or the file is stripped. This protects employees from malicious attachments included in a phishing attack from ever reaching the end user waiting for a chance to click.

For zero day threats reaching your network, WatchGuard APT Blocker executes the file in a cloud sandbox environment and analyzes its threat potential. Malicious files are quarantined, and system administrators are alerted of the threat.

But how can you protect those happy clickers?

WatchGuard DNSWatch leverages DNS-level detection to provide an additional layer of security to identify and stop malware infections. Malicious DNS requests are automatically detected and blocked, redirecting users to a safe place instead of the attacker. The Personal Touch component of this service provides detailed reports on the detected and blocked infection.

Best of all, the user making the request is redirected to a safe site that includes education information to reinforce the phishing 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. In the moment, users are much more receptive to advice, presenting an opportunity to enable new security features such as multi-factor authentication or enabling a password manager.



About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, and network intelligence products and services to more than 80,000 customers worldwide. The company's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for distributed enterprises and SMBs. 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.

WatchGuard

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

Part No. WGCE67085_032818