TROPHY PHISHING

Don’t Be The Next Trophy Hanging On The Hacker’s Wall

WatchGuard®

TABLE OF CONTENTS

WatchGuard®

INTRODUCTION

The truth is that the prevalence of phishing emails is for one simple reason – **they work.**

People keep clicking the links and downloading the files, so why would the hackers stop sending them?

Hackers are on the hunt for their next big trophy phishing catch, and they're waiting for you to take the bait. This eBook covers the top targets that hackers have in their sights, the bait and tactics they use to catch them and the defensive solutions you need to have in place to protect your employees and customers.

90%

of attacks start with a phishing email.

76%

of businesses report being a victim of a phishing attack in the last year.

(wombat security state of the phish)

WatchGuard

HACKERS FAVORITE LURES

Spear Phishing

Spear Phishing attacks take a much more targeted approach, requiring the hacker to study the victim before drafting the perfect email.

Executive Whaling

Targets the top executives and administrators, focused on siphoning off money from accounts or stealing confidential data.

Phishing

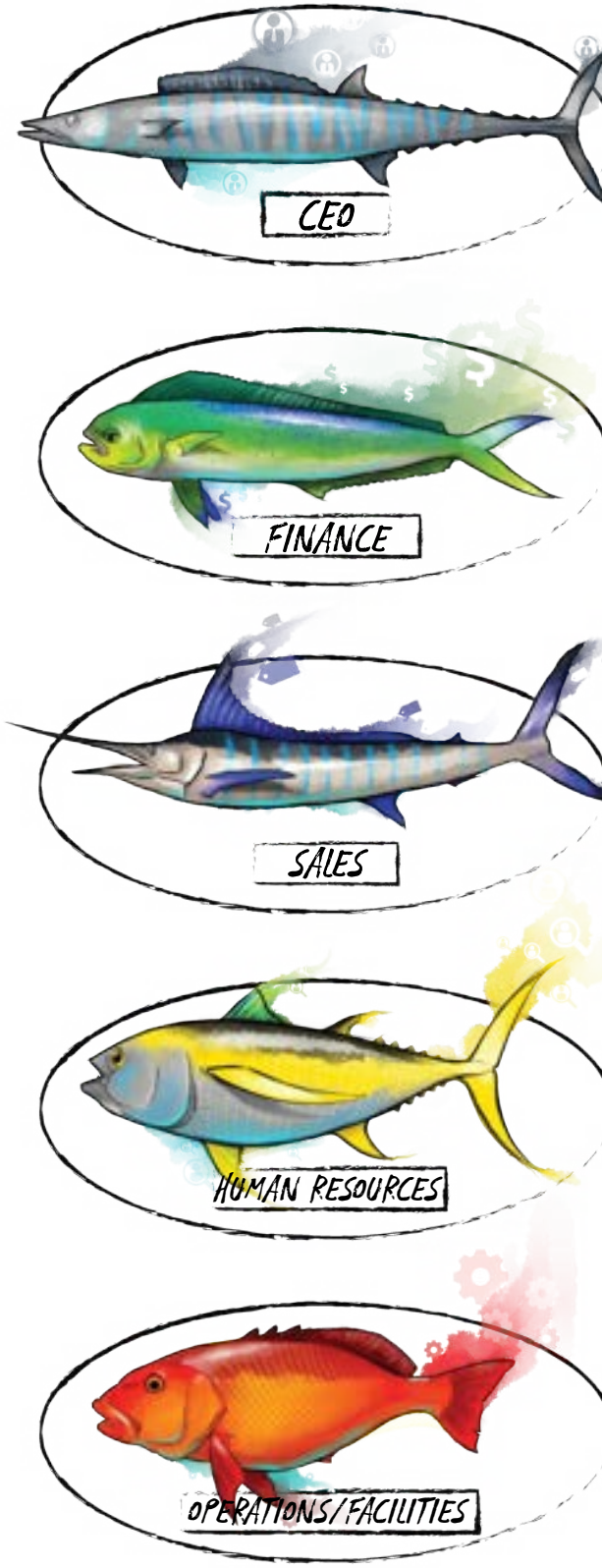
Phishing emails take a large sweep approach to attacking users and acquiring sensitive information.

Social Engineering

A way to mine information from social media sites to gain insight into how to craft the emails.

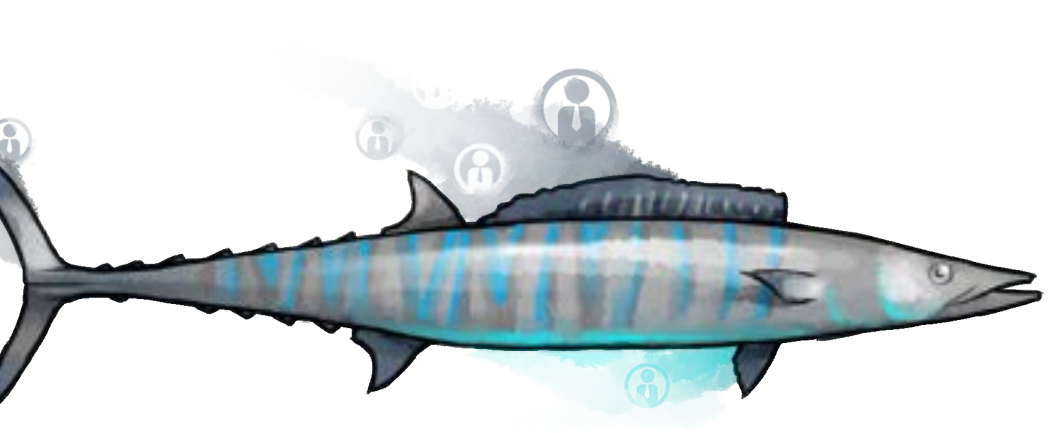
WHO ARE YOUR ORGANIZATION'S TOP TARGETS?

Every layer of your business has a trophy target just waiting to get caught on the hacker's hook. The best way you can protect them is to know the type of bait that the hacker will try to use and educate them on how to spot these threats when they cross their inbox. Learn more about the Top 5 Trophy Targets in your organization and the bait hackers will use against them.

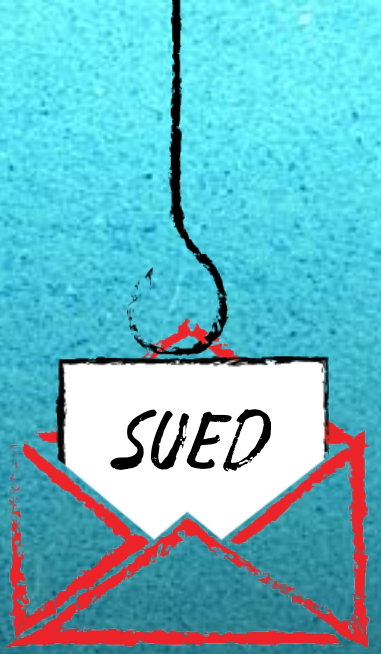


WatchGuard®

TROPHY TARGET: CEO



It's easy enough for hackers to find information on a company. Just a quick search of the company page, or social media sites like LinkedIn, makes it easy for them to find the names and email addresses of members of finance or legal teams. A simple email with a spoofed email address from a clerk on the legal team and a subject line with the threat of a lawsuit is sure to make even a CEO click any link.



CEO

Bait:

From legal -
"We're being sued"

TROPHY TARGET: FINANCE

If the CEO asks you to do something, it's usually in your best interest to do what they're asking (within reason). So, if you're on the finance team and the CEO asks you to transfer some funds, why would you second guess that? Hackers understand this, which is why they'll often spoof an email from the boss to get quick action from any employee. If they take the bait and click the transfer link, they'll be handing account information right over to the hacker.

FINANCE

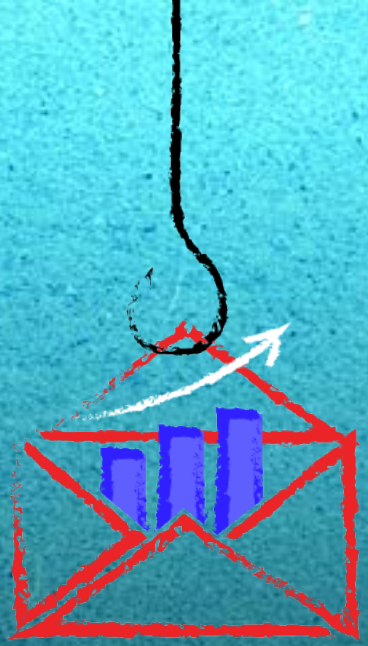
Bait:

From the CEO -

"I need you to transfer these funds!"

TROPHY TARGET: SALES

Sales people are used to fielding emails and phone calls from prospective clients and customers. They're eager to respond to any email that comes through that could be the next big catch. It's easy enough for a hacker to find a sales person's information (I mean… you know they're on LinkedIn) and they can be pretty confident that any email they send will at least be opened. A credential theft from these users would provide access to customer lists, pricing sheets, and confidential deal information. Stealing their accounts will also allow for a new phishing attack vector to members of the finance, management, and account teams, who would trust messages from the salesperson. This is the trophy phish that leads to many other great catches!



SALES

Bait:

From a prospect -

"I'm your next big sale!"

TROPHY TARGET: HR

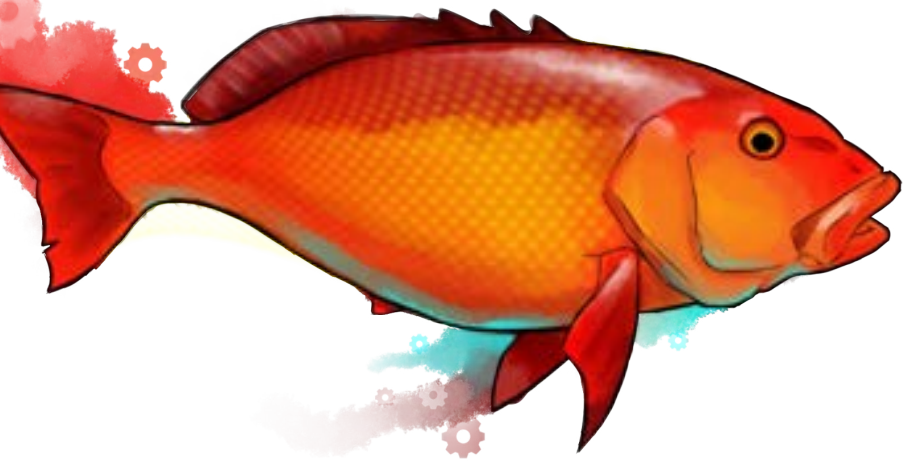
Regardless of the standard practices, members of your human resources team are used to receiving resumes via email. And while they might not open every one, hackers know that if they craft the right email there's a chance that the HR team could open the email and download the attachment. From there, the hacker has access to sensitive employee information, including social security numbers, addresses, phones numbers, even the details of emergency contacts. They could even get access to healthcare information or 401K providers which can line them up for the next hack against your organization.

HUMAN RESOURCES

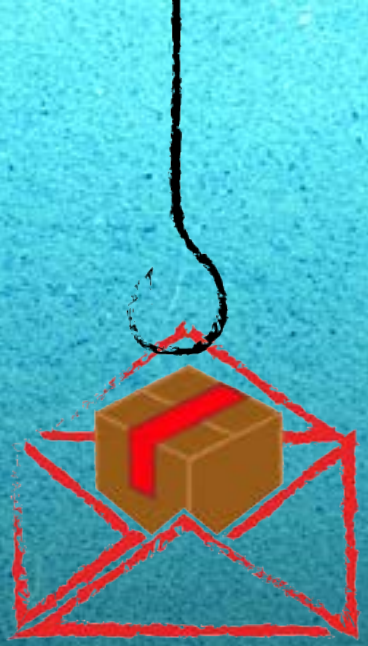
Bait:

From a prospective employee -
"Hire me!"

TROPHY TARGET: OPERATIONS



Shipping attachments for UPS and FedEx orders are another common way that attackers gain access to your business. Operations and facilities team members (or even regular staff that often receive shipments) are used to receiving these types of emails with an attachment containing important shipping information. Subject lines like "missing package" or "issue with delivery" are certainly going to get their attention. Hackers know that even if this part of your organization isn't expecting a shipment, they're still pretty likely to open that email and click that link or download that attachment.



OPERATIONS/ FACILITIES

Bait:

From a shipping company -

"Your package is missing"

HOW TO KEEP OFF THE HACKER'S HOOK

While these phishing attacks can you leave you swimming away towards calmer waters, having the right defenses in place can keep you, your employees and your customers protected. WatchGuard offers a robust portfolio of security solutions to ensure that you're secure at every layer and against every type of attack.

WatchGuard®

WATCHGUARD TOTAL SECURITY SUITE

Layered defense across your entire organization.

Phishing attacks often target different parts of your business in a variety of ways. This requires security at every layer of your organization against known, unknown and even evasive threats. WatchGuard Total Security Suite protects your business from phishing attacks whether they involve malicious links or attachments. Here's how:

WatchGuard DNSWatch monitors DNS traffic and blocks access to known malicious sites. So when a user receives a phishing email and clicks the link trying to point them to a malicious site, DNSWatch steps in to make sure that the user isn't able to access the dangerous site. For bonus points, this service redirects users to a safe page that refreshes them on the warning signs to look out for with a phishing email.

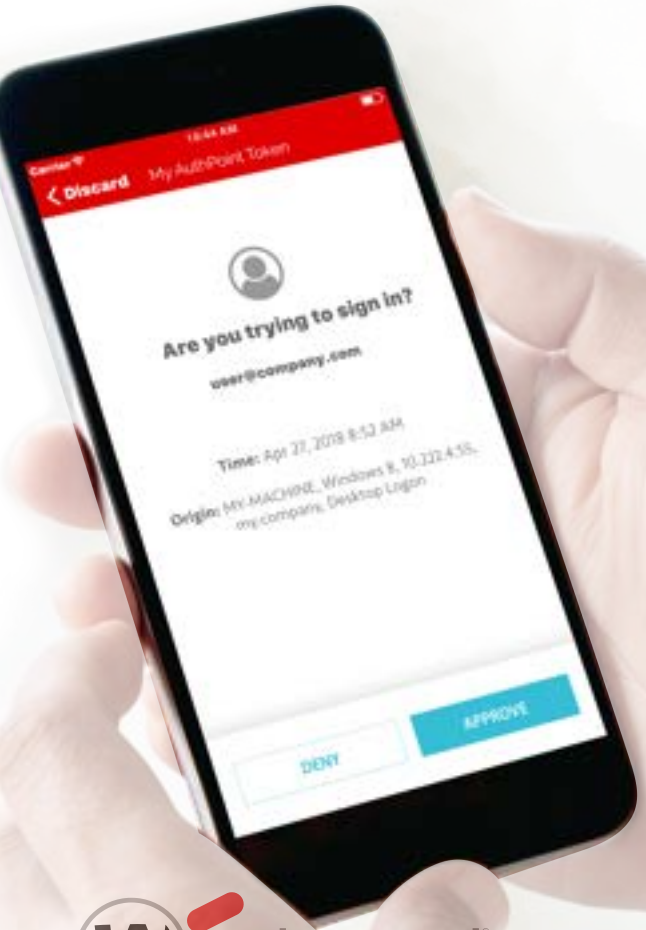
WatchGuard APT Blocker detonates suspicious files detected on the network and host in a virtual environment to determine if they have malicious intent. If the file is deemed malicious, it is quarantined from the user. This ensures that any phishing emails containing attachments will be detonated and determined malicious before ever being opened on an user's device.

WatchGuard Threat Detection & Response (TDR) provides protection against ransomware attacks. Should an employee receive a phishing email that contains ransomware, the Host Ransomware Prevention (HRP) component of TDR will detect the threat and remediate it before file encryption takes place.

WatchGuard

WATCHGUARD AUTHPOINT

Protection against stolen credentials



Should a hacker gain access to your organization and find a way to steal user credentials, you need a way to ensure that even if they get those credentials they won't get very far. Multi-factor authentication (MFA) requires that a user have something they know, something they are or something they have before they can gain access.

WatchGuard AuthPoint™ not only helps customers to reduce the likelihood of data breaches arising from lost or stolen credentials, but we deliver this solution entirely from the Cloud for easy set-up and management even with limited staff. AuthPoint goes beyond traditional 2-Factor Authentication (2FA) by leveraging innovative ways to positively identify users – such as with our Mobile Device DNA approach. And our large ecosystem of 3rd party integrations means that customers can consistently deploy AuthPoint protection to access the network, VPNs, Cloud applications – wherever it's needed. With WatchGuard AuthPoint, even if the hacker steals your password, they won't be able to access your data and applications.

WatchGuard

PROTECT YOUR BUSINESS • PROTECT YOUR ASSETS • PROTECT YOUR PEOPLE

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.

Global Headquarters
United States
Tel: +1.800.734.9905
Email: sales@watchguard.com

European Headquarters
The Netherlands
Tel: +31(0)70.711.20.85
Email: sales-benelux@watchguard.com

APAC & SEA Headquarters
Singapore
Tel: +65.3163.3992
Email: inquiry.sea@watchguard.com

©2018 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, AuthPoint, DNSWatch, Dimension and Firebox are trademarks or registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other tradenames are the property of their respective owners.

Part No. WGCE67116_080118