



# Your Ultimate Guide to Phishing Mitigation

**Roger A. Grimes**  
**Data-Driven Security Evangelist**  
**[rogerg@knowbe4.com](mailto:rogerg@knowbe4.com)**

# About Roger



**Roger A. Grimes**  
**Data-Driven Defense Evangelist**  
**KnowBe4, Inc.**

**Twitter: @rogeragrimes**

**LinkedIn: <https://www.linkedin.com/in/rogeragrimes/>**

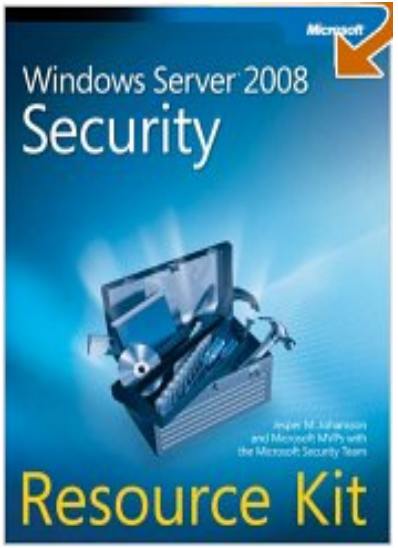
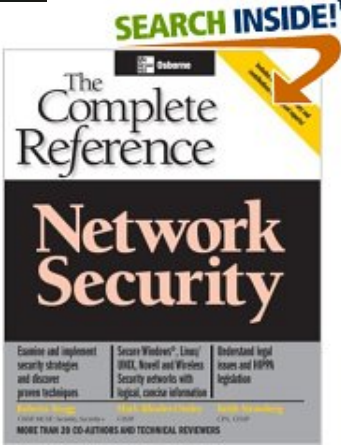
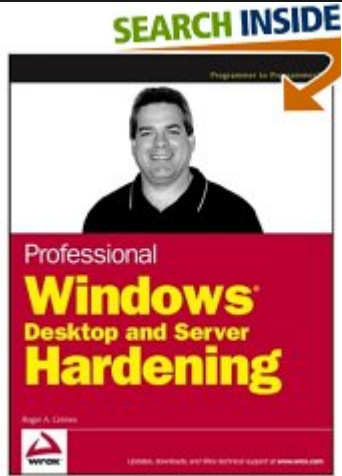
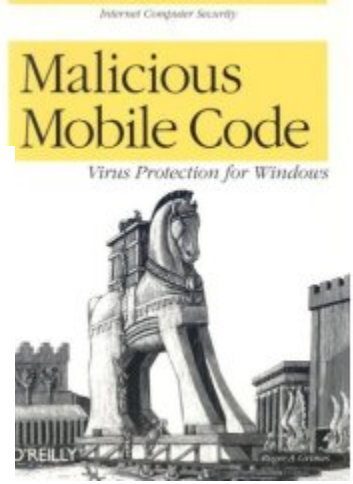
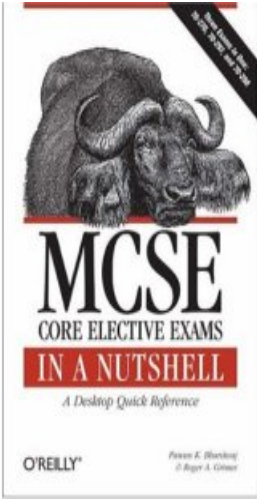
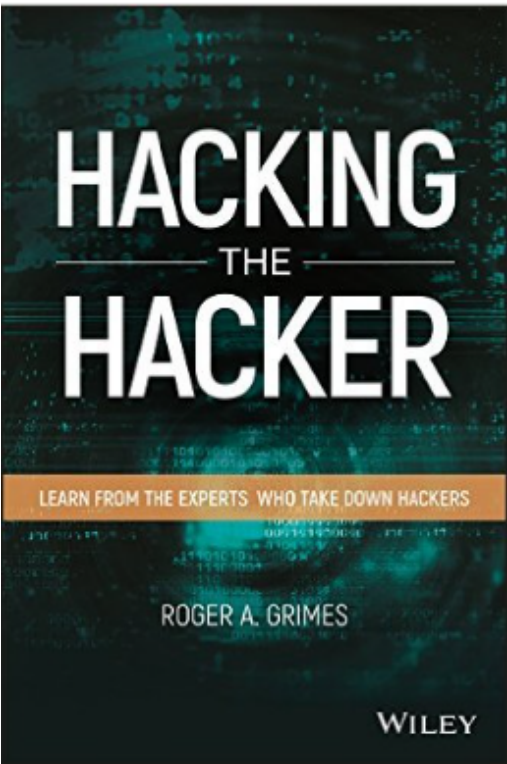
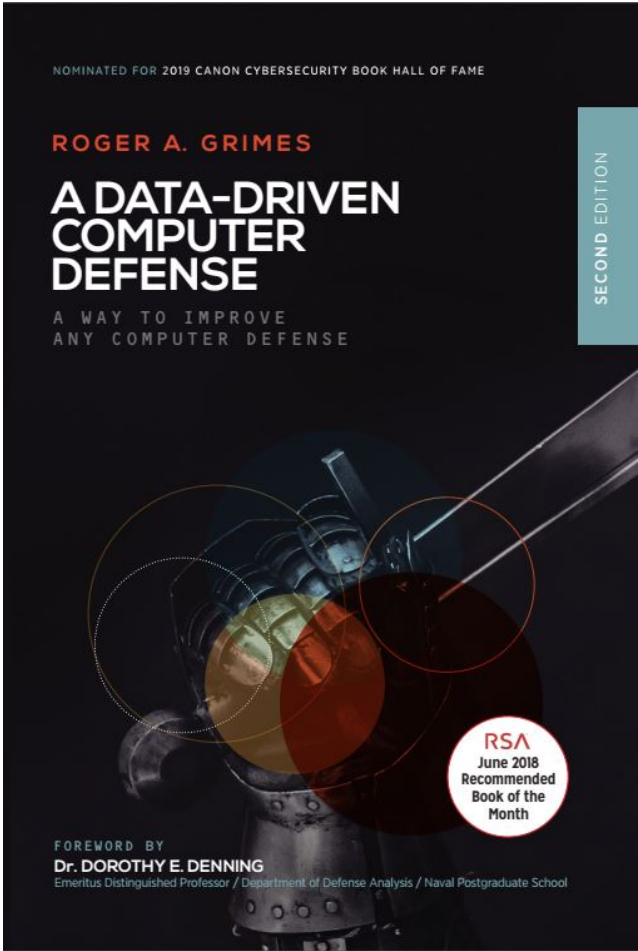
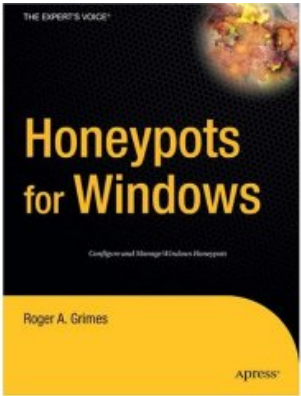
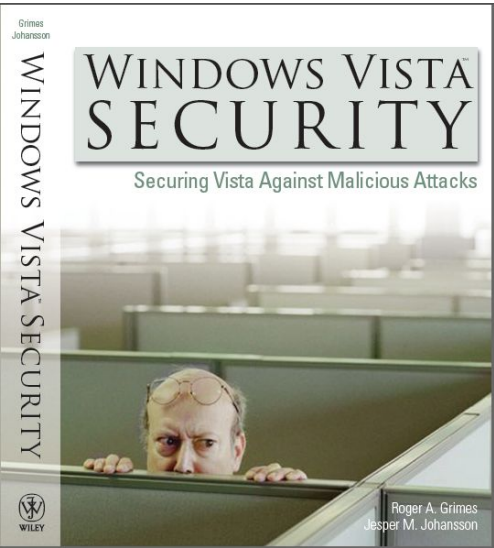
- 30 years plus in computer security
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 10 books and over 1,000 magazine articles
- *InfoWorld* and *CSO* weekly security columnist since 2005
- Frequently interviewed by magazines (e.g. Newsweek) and radio shows (e.g. NPR's All Things Considered)

## **Certification exams passed include:**

- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada



# Roger's Books



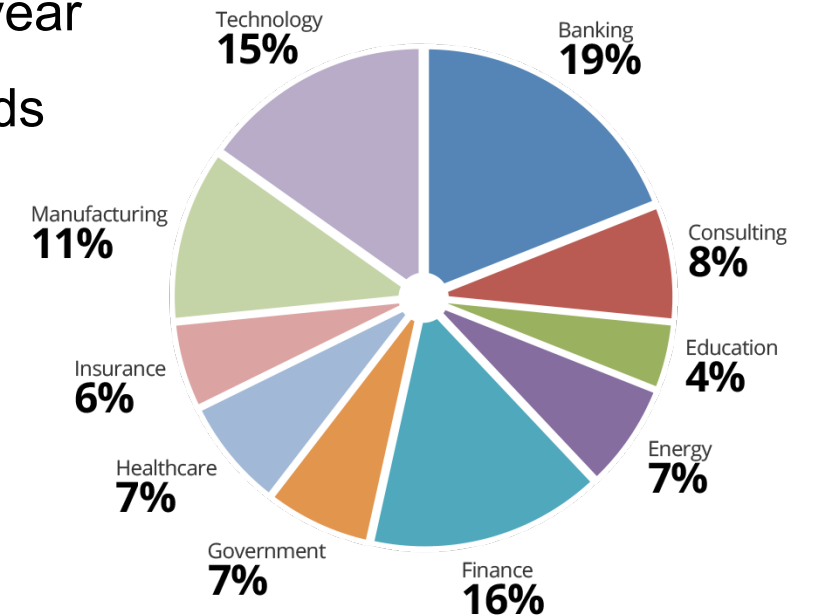
RSA June 2018 Book of the Month  
Harvard Business Review  
2019 Canon Cybersecurity Book Hall of Fame nominee





# KnowBe4, Inc.

- The world's most popular integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex-antivirus, IT Security pros
- 200% growth year over year
- We help tens of thousands of organizations manage the problem of social engineering





# Today's Presentation

## All Things Phishing Mitigation

- Developing a Comprehensive, Defense-in-Depth Plan
- What Policies You Need
- Technical Controls
- Implementing Fantastic Security Awareness Training
- Ins and Outs of Cybersecurity Insurance
- Other Real-Life Hints

# Today's Presentation

## All Things Phishing Mitigation - Goals

- To expose attendees to all the possible defenses that any organization could be doing to fight phishing
- To help attendees close any critical gaps in their own phishing defenses
- Not intended to be a detailed talk about each possible defense

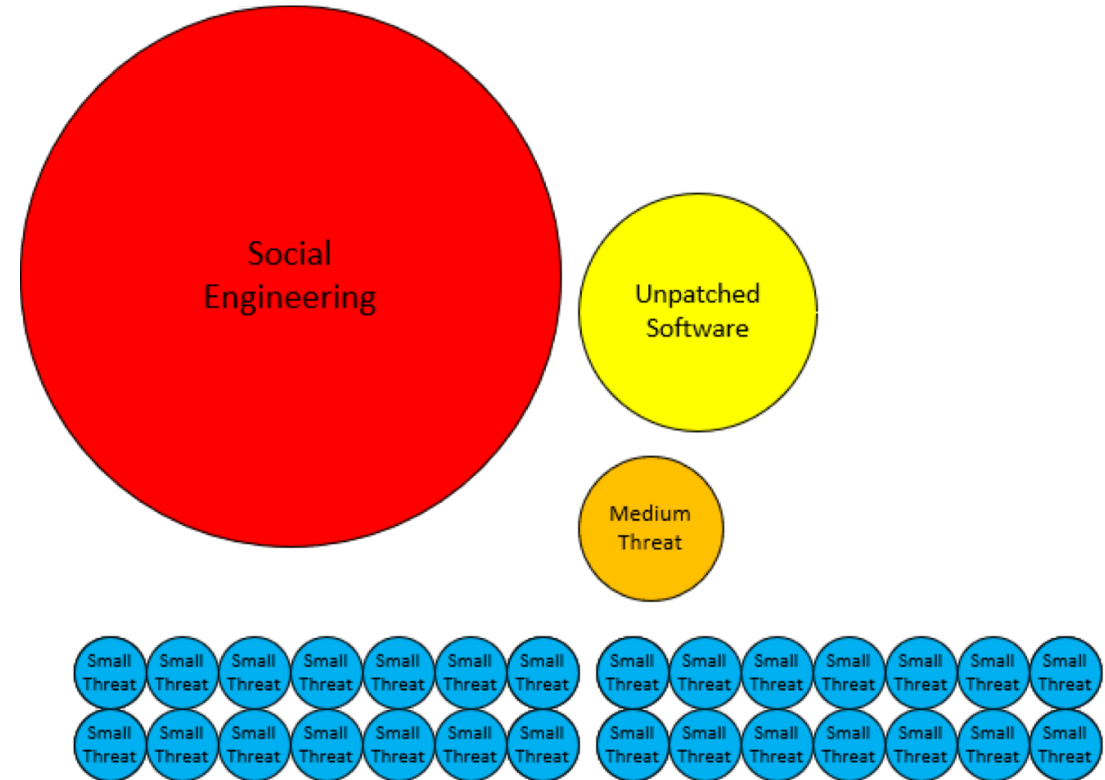


# Biggest Initial Breach Root Causes for Most Companies

- Social Engineering
- Unpatched Software

## Preventative Controls

- Technical
- Training



**Social engineering is responsible for 70% - 90% of all malicious data breaches**

# Agenda

- Developing a Comprehensive, Defense-in-Depth Plan



# Defense In Depth Plan

## Summary

- Policy and Documentation
- Selection and Implementation of Technical Controls
- Security Awareness Training
- Other Security Checks
- Cybersecurity Insurance?

# Agenda

- Needed Policies



# Defense In Depth Plan

## Policy and Documentation

- **Acceptable Use Policy** – (AUP) Every user reads and signs when hired and annually thereafter
  - More general
- **Specific Phishing Mitigation Policies**
  - Documented, education, testing
  - More specific
  - More frequently – once a month
- **Training docs and content**

# Defense In Depth Plan

## Acceptable Use Policy

- Educate users and vendors about what is allowed and not allowed regarding IT devices and services, including personal responsibilities
- There are tons of examples on the Internet
- Good example:  
[https://www.getsafeonline.org/themes/site\\_themes/getsafeonline/download\\_centre/Sample\\_Acceptable\\_Usage\\_Policy.pdf](https://www.getsafeonline.org/themes/site_themes/getsafeonline/download_centre/Sample_Acceptable_Usage_Policy.pdf)



# Defense In Depth Plan

## Acceptable Use Policy – Phishing Mitigation Section

- Needs to include phishing policies and guidelines
  - Unfortunately, most do not include phishing-related language
    - Need to change with the times
    - Should be reviewed and updated annually, just before all employees are told to read and sign again
  - Needs to include major/general phishing mitigation policies, and a link to the more detailed document(s)

# Defense In Depth Plan

## Acceptable Use Policy – Phishing Mitigation Section

- Employee monitoring section
  - May need to be updated to account for simulated phishing test results
  - Some privacy laws/guidelines may consider admins looking at simulated phishing test results for individual users as an unlawful privacy invasion if the employee is not made aware of

# Defense In Depth Plan

## Specific Phishing Mitigation Policies

Examples:

**Stated Policy Objective:** “Acme Organization recognizes that one of the most popular ways any organization can be compromised is social engineering and phishing...”



# Defense In Depth Plan

## Specific Phishing Mitigation Policies

Examples:

**Risks** include: unauthorized system access, denial of service, data exfiltration, reputation issues, attacks against our employees and customers, stolen IP, fines, financial harm, etc.

- May already be included in general security policy

# Defense In Depth Plan

## Specific Phishing Mitigation Policies

Examples:

### Definitions

- Include: Social Engineering, Phishing, Spear Phishing, Ransomware, CEO Wire Fraud, Smishing, Vishing, patching, etc.

# Definition Example: What is Phishing?

- The process of attempting to acquire sensitive information such as usernames, passwords and credit card details or create a desired action by or from a victim by masquerading as a trustworthy entity
- Simply put - a “con”, criminal-intent
- Often done using in-person, email, IM, SMS, phone, etc.
- AKA phishing, spear phishing, spamming, vishing, etc.
- Emails/messages/SMS/Voice calls claiming to be from friends, co-workers, popular social web sites, banks, auction sites, or IT administrators are commonly used to lure the unsuspecting public.

# Defense In Depth Plan

## Specific Phishing Mitigation Policies

Examples:

### Common Ways to Recognize Social Engineering

- Common Phishing Red Flags
  - Unexpected subjects, email addresses
  - Email and links incongruent to display names
  - Request for logon credentials



# Social Engineering Red Flags

## FROM

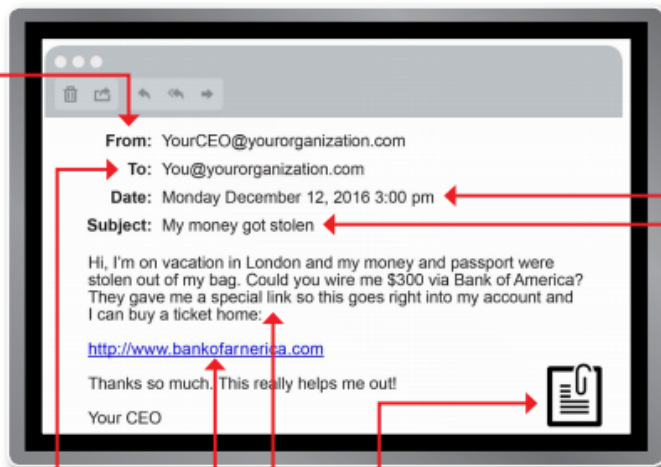
- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- I **don't know the sender personally** and they **were not vouched for** by someone I trust.
- I **don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

## TO

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

## HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big red flag**.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, [www.bankofarnerica.com](http://www.bankofarnerica.com) — the "m" is really two characters — "r" and "n."



## DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

## SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?

## ATTACHMENTS

- The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt file**.

## CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

# Defense In Depth Plan

## Specific Phishing Mitigation Policies

Examples:

### What to Do When a Phish Is Detected

- Don't Open/Click on Links
- Call Sender, when in doubt
- Report, Call
  - Simplify - Report button (ex. Phish Alert button)



# Defense In Depth Plan

## Specific Phishing Mitigation Policies

Examples:

### **Tell Employee What to Do When One Is Detected**

- What actions to take
- You want to create a culture of acceptance for reporting possible phishes
- Remind people they do not get in trouble for reporting possible phishes, reporting late, etc.

# Defense In Depth Plan

## Specific Phishing Mitigation Policies

Examples:

### What to Do When Someone Is Successfully Phished

- Incident Response activities
- We believe in “more carrot and less stick”
- Required education
- Tie to annual review
- Different requirements for a greater number of “misses”



# Defense In Depth Plan

## Specific Phishing Mitigation Policies

Examples:

### **What Is IT's Response to a Successful Phish?**

- What Is Incident Response Plan for Phishing?
- Gather Initial Information
- Minimize Further Damage
- Forensics
- Future Prevention
- Need to Update Policies or Training?

# Defense In Depth Plan

## Specific Phishing Mitigation Policies

Examples:

### When Does a “Failed” Phishing Attempt Need to Be Investigated?

- What type of events create IR even for failed phishes?
- Example: Numerous reports of same phish, same origination point/country
- If you find one successful phish that led to a dropper file and there were many attempts, check for dropper file on all computers

# Defense In Depth Plan

## Specific Phishing Mitigation Policies

Examples:

### Security Awareness Training Notification

- Let employee know that it is done
- How it is done
  - Educate about simulated phish testing campaigns
- How often it is done
- What are the official training methods and from whom

# Defense In Depth Plan

## Specific Phishing Mitigation Policies

Examples:

### General/Misc

- Users Should Hover Over All URL Links to Verify
- Don't Install Unauthorized Software
- Never give logon credentials in response to email or call
  - Use MFA when possible



# Defense In Depth Plan

## Specific Phishing Mitigation Policies

Examples:

### To Prevent CEO Wire Fraud Phishing

- Update policy to say that all unexpected requests for money, gift cards, invoice payments, etc., **MUST** be confirmed verbally with the requestor (at least above a certain threshold)

# Defense In Depth Plan

## Other Policies

- Ransom – Pay or Not Pay?
- Disaster Recovery Plan/Business Continuity Plan
- Vendor Risk Management
- Partner Communication Plan

# Defense In Depth Plan

## Any Policy

- **Important: Any adds/deletes/changes to any policies or documents need to be reviewed by management and legal before implementing**

# Agenda

- Cybersecurity Insurance



# Cybersecurity Insurance

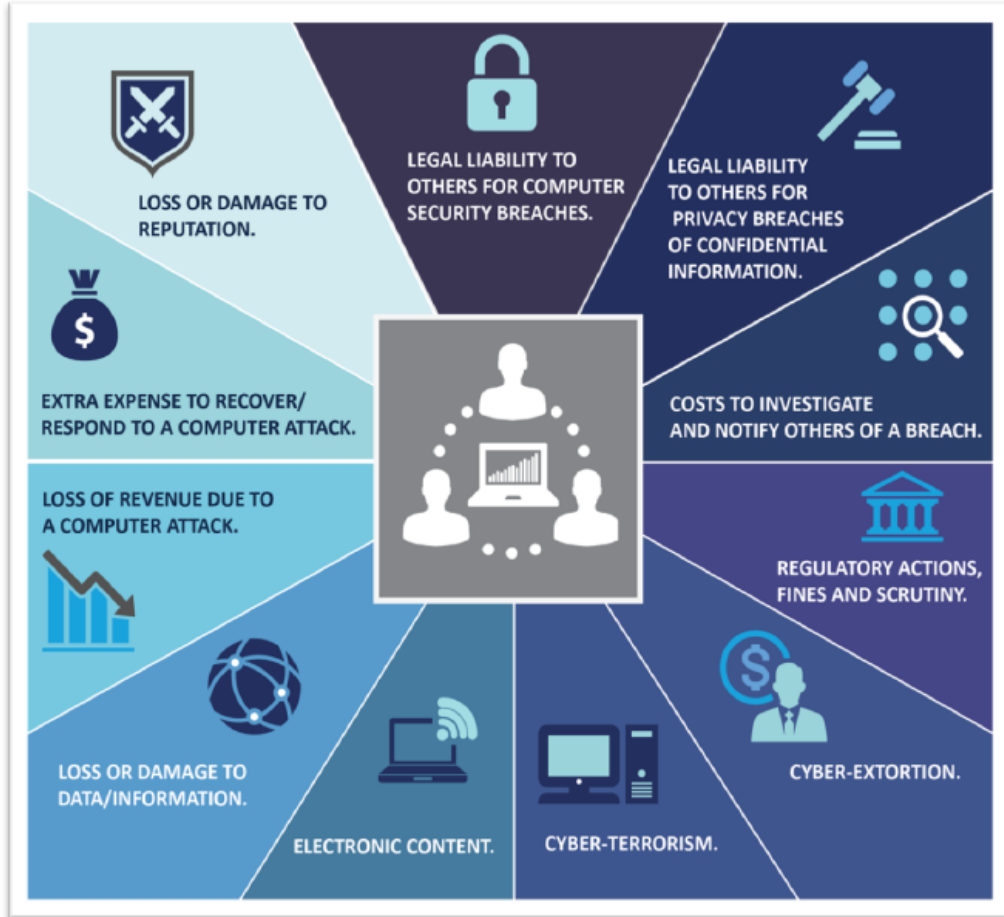
## Overview

Insurance to cover damages from cybersecurity events

- Excluded from most general insurance policies
- Over 170 companies offer it, Top 5 firms write over 50% of policies
- Currently 1/3<sup>rd</sup> of companies have it
  - Mostly large companies
- Fairly low cost (1%-3% the cost of most other business insurance policies)
- Lots of “outs” (i.e. cyberwarfare, etc.)
- Very profitable for insurance companies: They only payout 1/3 of premiums

# Cybersecurity Insurance

## What is Covered in a Cyber Policy?



### First Party

2/3rds of claims

- Event Management
- Cyber Extortion
- Data Restoration
- Network Business Interruption
  - system failure & security incident
- Other: social engineering, reputational harm, bricking

### Third Party

- Privacy Liability
- Network Security Liability
- Privacy Regulatory Defense Costs
- Media Liability

# Cybersecurity Insurance

## Pricing

Based on:

- Max. payout of policy
- Number of records a company has
- Meeting compliance requirements (usually just a verbal or paper checklist of binary questions)
- A general idea of your cybersecurity maturity and culture
- What cybersecurity incidents are included/excluded
- Ave. Claim Size in 2017 was \$56,668

# Cybersecurity Insurance

## Know What Is Included/Excluded

- Is there a coverage reduction for social engineering attacks?
  - Example: \$50M policy limited to \$200K for phishing attacks
- Are Ransomware Payments Included?
- Are CEO Wire Fraud events included, where employee accidentally helped?
- Are intentional insider events cover?
- What assets are covered? (SCADA, A/C, etc.)

# Agenda

- Technical Controls

# Technical Controls

## Where

- On Network Edge/Ingress/Egress Points
  - On Host
  - On Cloud Service
- 
- Inbound Traffic
  - Outbound Traffic



# Technical Controls

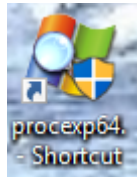
## Malware Mitigation

- Antivirus
- Endpoint Detection & Response (EDR)
- Google Virus Total (70+ AV engines, scan on submit)
- Intrusion Detection
- Firewall

# Check Yourself Against 70+ AV Engines

## Process Explorer

- [www.sysinternals.com](http://www.sysinternals.com)
- Free tool from Microsoft
- Can be used to compare all running processes against 60+ antivirus scanners at once on Virus Total
- Doesn't slow your system down
- Highly accurate, if you ignore the numerous 2/69 false-positives



Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-OI9DB93\Roger G]

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
WindowsSensor.exe		7,784 K	6,356 K	29472	CrowdStrike Windows Sensor	CrowdStrike, Inc.	Unknown
WindowsSensor.exe		7,772 K	7,864 K	39408	CrowdStrike Windows Sensor	CrowdStrike, Inc.	Unknown
OUTLOOK.EXE	2.17	795,152 K	430,708 K	26344	Microsoft Outlook	Microsoft Corporation	Unknown
conhost.exe	< 0.01	5,648 K	1,492 K	7660	Console Window Host	Microsoft Corporation	1/68
conhost.exe		5,436 K	1,388 K	11308	Console Window Host	Microsoft Corporation	1/68
winlogon.exe		2,728 K	3,708 K	1308	Windows Logon Application	Microsoft Corporation	0/69
vmware-authd.exe	< 0.01	6,568 K	4,680 K	4812	VMware Authorization Service	VMware, Inc.	0/69
vmnetdhcp.exe		7,448 K	960 K	4820	VMware VMnet DHCP service	VMware, Inc.	0/69
ScanToPCActivationApp.exe		6,668 K	7,508 K	13148	ScanToPCActivationApp	HP Inc.	0/69
NinjaRMMAgent.exe	0.01	92,304 K	42,248 K	7140	Ninja RMM Agent Worker	Ninja MSP	0/69
Microsoft Edge.exe	0.05	227,416 K	161,808 K	13248	Microsoft Edge	Microsoft Corporation	0/69
LMS.exe		4,380 K	4,592 K	3640	Intel(R) Local Management ...	Intel Corporation	0/69
DDVCollectorSvcApi.exe		1,836 K	1,804 K	20804	Dell Data Vault Data Collect...	Dell Inc.	0/69
DataExchangeHost.exe		4,972 K	10,456 K	11424	Data Exchange Host	Microsoft Corporation	0/69
WUDFHost.exe		4,556 K	6,120 K	1036	Windows Driver Foundation ...	Microsoft Corporation	0/68
WINWORD.EXE		196,020 K	222,776 K	1232	Microsoft Word	Microsoft Corporation	0/68
WavesSvc64.exe		46,904 K	9,972 K	11644	Waves MaxxAudio Service ...	Waves Audio Ltd.	0/68
svchost.exe		1,000 K	408 K	840	Host Process for Windows S...	Microsoft Corporation	0/68
svchost.exe	0.05	26,872 K	31,312 K	436	Host Process for Windows S...	Microsoft Corporation	0/68

# Technical Controls

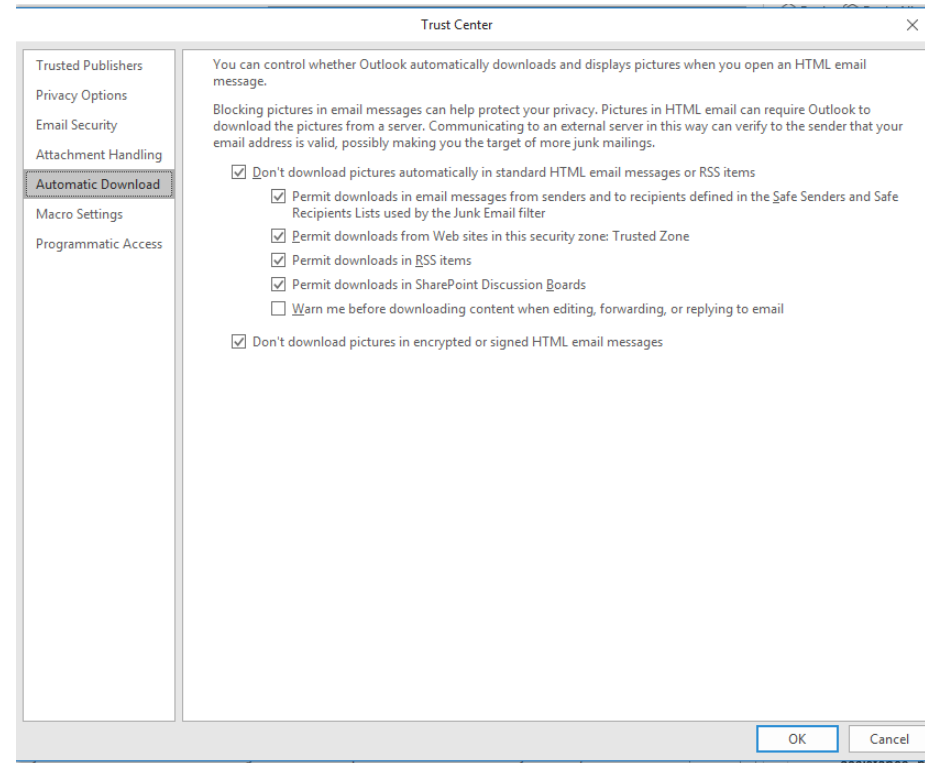
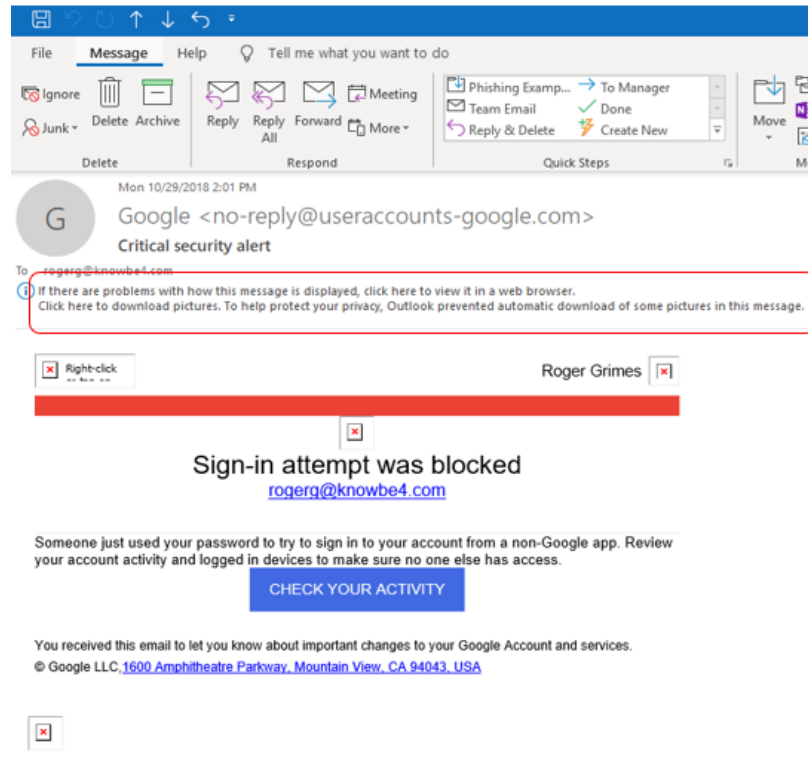
## Email-Specific

- Email Client Protections
  - Strongly configured email protections

# Technical Controls

## Email-Specific

- Email Client Protections



# Technical Controls

## Email-Specific

- Email Client Protections
  - Strongly configured email protections
- Browser Protections
- Email Service Provider Protections

# Technical Controls

## Global Phishing Protection Standards

- Sender Policy Framework (SPF)
- Domain Keys Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting and Conformance (DMARC)
- All work using TXT DNS records



# Technical Controls

## Sender Policy Framework (SPF)

- Designed to prevent sender email address spoofing by receiver verifying the IP address of the mail server the email arrived from matches a list of allowed IP addresses designed by domain's admins
- Relies on SPF/TXT records in DNS
  - example.com. IN TXT "v=spf1 -all"
  - example.com. IN TXT "v=spf1 a ip4:192.168.1.1 ~all"
- Sender must have it enabled
- Receiver checks

# Technical Controls

## Domain Keys Identified Mail (DKIM)

- Designed to prevent sender email address spoofing by receiver verifying the digital signature of the mail server domain sent with each email
- Relies on DKIM/TXT records in DNS
- Sender must have public/private key pair
- Server signs each outgoing email
- Receiver side: All validation is done before email gets to end-user

# Technical Controls

## Domain Keys Identified Mail (DKIM)

Example DKIM Email Header

- `_domainkey.example.com. 600 IN TXT "v=DKIM1\;  
p=eGGfMA0GCSqHSIb3DQEBAQUAA4GNADCBiQKBgQC1TaNgLISyQMN  
WVLNLvyY/neDgaL2oqQE8T5iIlKqCgDtFHc8eHVAU+nlcaGmrKoDMw9dbgi  
Gk1ocgZ56NR4ycfUHwQhvQPMUZw0cveel/8EAGoi/UyPmqfcPibytH81NFtT  
MAxUeM4Op8A6iHkvAMj5qLf4YRNsTkKAV;"`

# Technical Controls

## DMARC

- Sender can indicate whether they use SPF and/or DKIM, which the receiver can verify and rely on, and how a receiver should treat failed messages
- TXT IN  
"v=DMARC1;p=none;sp=quarantine;pct=100;rua=mailto:dmarccheck@example.com;"

# Technical Controls

## Global Phishing Protection Standards

- Sender Policy Framework (SPF)
- Domain Keys Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting and Conformance (DMARC)
- None of them are perfect, but they do help
- You should implement
- Be care of requiring (i.e. reject), instead use quarantine

# Technical Controls

## Filtering

- Content Filtering
  - On email
  - On Internet browsing content
- Spam Filters
- Phishing Filters
- Email Filtering



# Technical Controls

## Filtering

- Block Malicious File Attachments
- Block Outbound File Links and Protocols
  - Example: <file:///www.badguy.com/doc.html>
  - <https://www.csoononline.com/article/3333916/windows-security/i-can-get-and-crack-your-password-hashes-from-email.html>

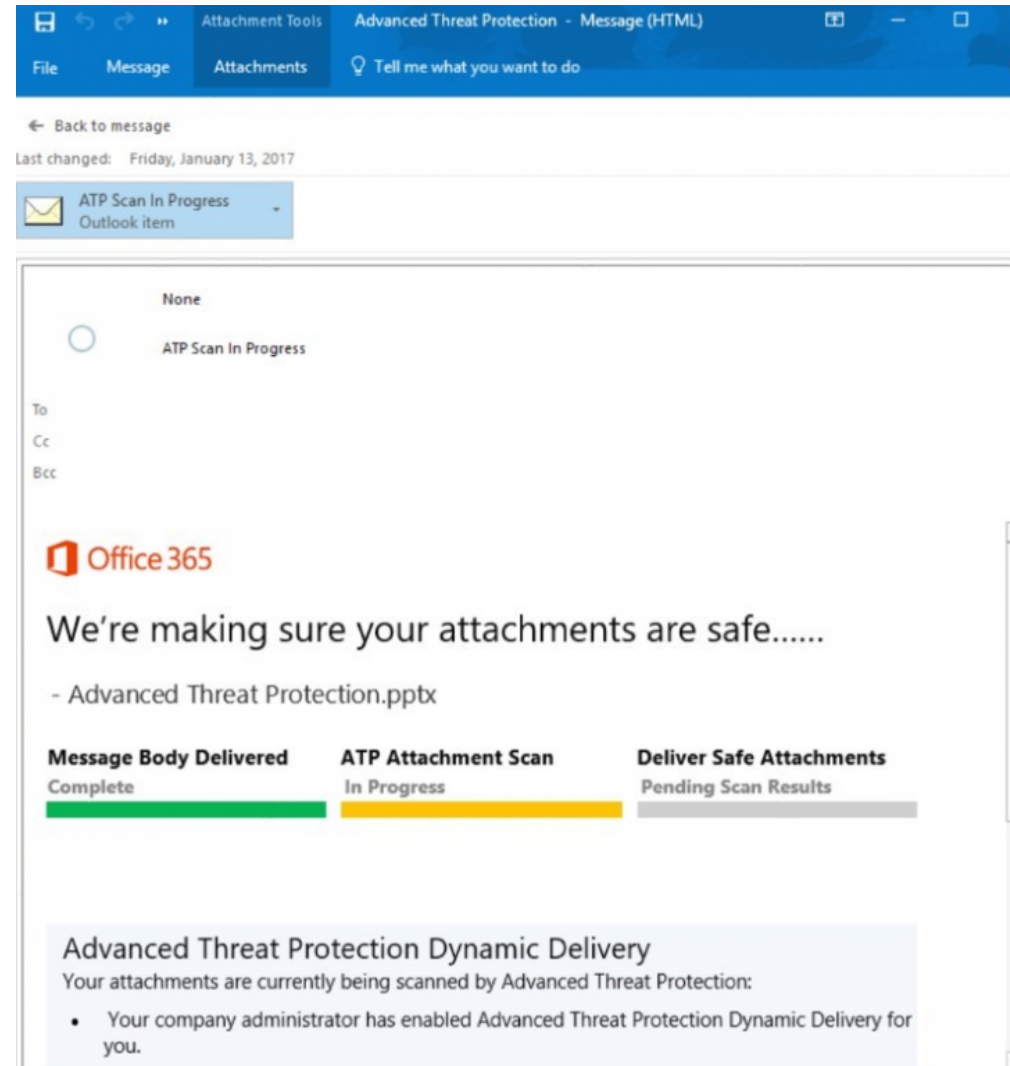
# Technical Controls

## File Attachment and URL Detonation

- All/Potentially malicious file attachments/URLs in emails are opened and examined for badness before sending onto user
- AKA Sandboxing
- Ex Vendors/Products: Microsoft ATP Safe Links/Safe Attachments, Barracuda, Proofpoint, Blue Coat, FireEye

# Technical Controls

## File Attachment and URL Detonation



# Technical Controls

## Blacklisting

- Lists of confirmed or potentially malicious domains, which can be used to block email, DNS queries, etc.
- Some orgs block whole countries (e.g. Russia, China, etc.)
  - I don't recommend this strategy, but I have seen it work
- Blacklist Master (<https://www.blacklistmaster.com/blacklists>) (108 BLs)
- Example Vendors/Products: Spamhaus, DNSBL, Ospam, Google Safe Browsing

# Technical Controls

## Reputation Services

- Related to blacklisting, but more intelligent and dynamic
- Example Vendors/Products: Crowdstrike, Microsoft Windows Defender Application Guard, Google

# Technical Controls

## Network Traffic Pattern Analysis

- Analyzes network traffic patterns looking for signs of unauthorized activity
- Examples: Huge files being transferred to a foreign country you don't do business with, a server connecting to lots of other servers, etc.
- Example Vendors/Products: FireEye, Crowdstrike, Aruba, Cisco Stealthwatch, Corelight, Bro



# Agenda

- Fantastic Security Awareness Training

# The KnowBe4 Security Awareness Program WORKS



## Baseline Testing

Use simulated phishing to baseline assess the Phish-prone™ percentage of your users.



## Train Your Users

The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.



## Phish Your Users

Best-in-class, fully automated simulated phishing attacks, hundreds of templates with unlimited usage, and community phishing templates.



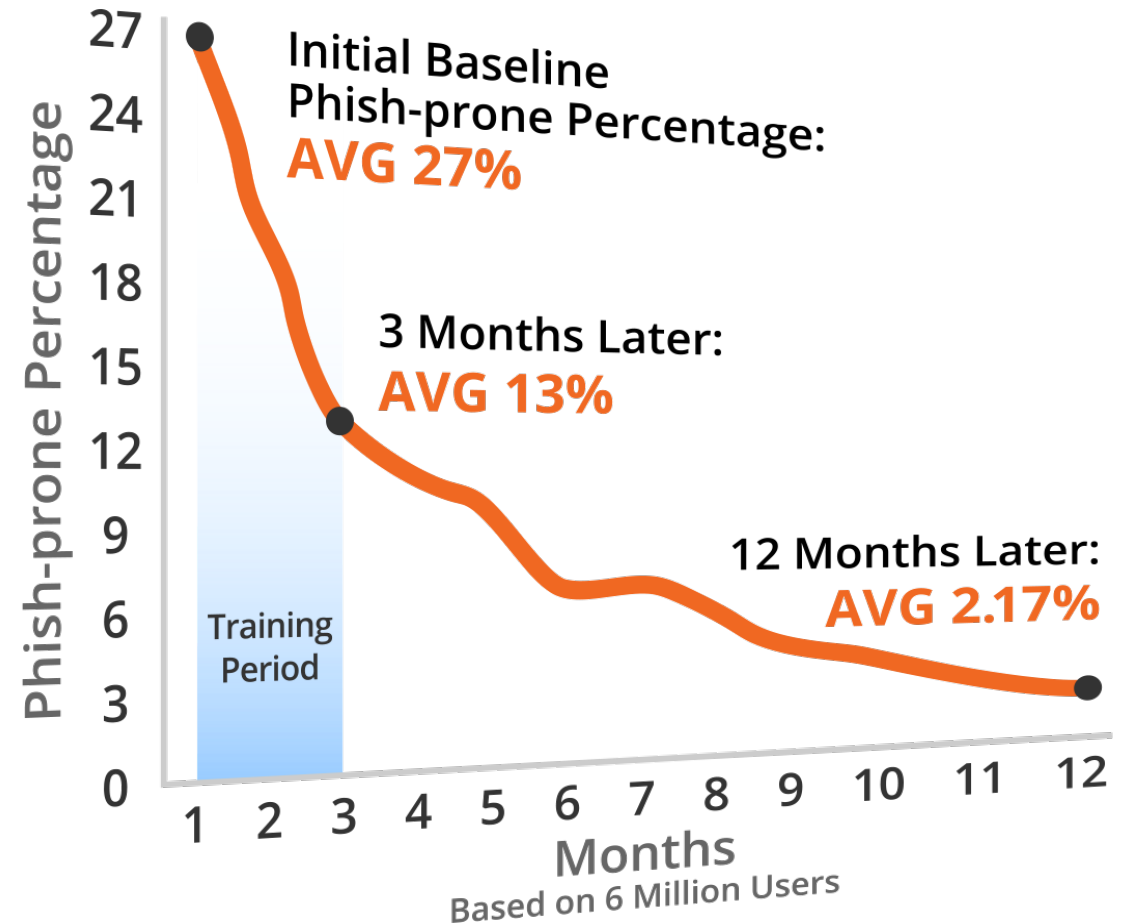
## See the Results

Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!

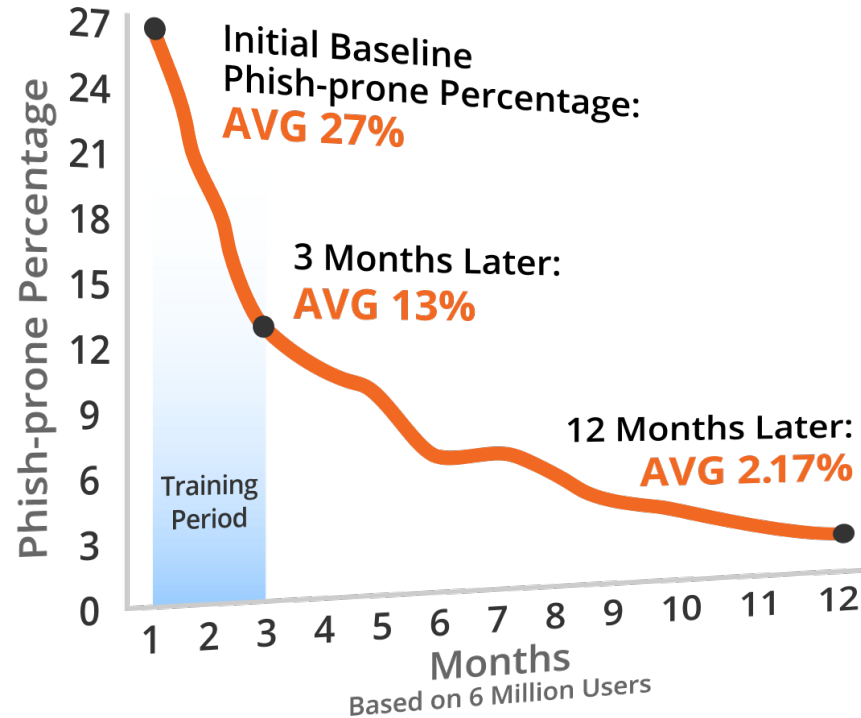


# Security Awareness Training Program That Works

- Drawn from a data set of **over six million users**
- Across **nearly 11K organizations**
- Segmented **by industry type** and **organization size**
- **241,762** Phishing Security Tests (PSTs)



# Metrics, Videos, Posters, Gamification, and more



Your metrics and reporting help tell your story.

SHALL WE PLAY A GAME?

Consider using gamification and incentives to encourage friendly competition across departments.

Make everything reinforce your point and purpose

# It's Not About Intelligence

There's a reason it's called Security Awareness Training

- IQ is not a good indicator of how likely you are to be successfully phished
  - Nobel Physics prize winners have been phished out of millions of dollars
- Whether or not you are aware of a particular type of social engineering is the biggest predictor of phishing success or failure
- So train, train, train

# Security Awareness Training Cycle

- When Hired
  - Acceptable Use Policy
  - Longer, Broader Training
- Ongoing
  - Monthly simulated phishing attacks
  - Immediate training when a test is failed
  - Ongoing shorter trainings
- Annual – longer training
- More Training As Needed

# Make It Relevant

- Per Group, Per Role
  - You want different training for your executives versus your front-line employees
- Times, Season, Events of the Year
  - Different seasons and events generate different types of phishing
- Mix in general topics
- Not just email
- Not just to protect work scenarios only



# Make It Relevant

## Spear Phish Your Employees

Don't let all the spear phishing testing be by the hackers

- Any public information is fair game
- Private information can be fair game
- Use a mix of general and spear phishing to test and train your employees

# Give “Red Flags” Training

## Social Engineering Red Flags



### FROM

- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- I **don't know the sender personally** and they **were not vouched for** by someone I trust.
- I **don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.



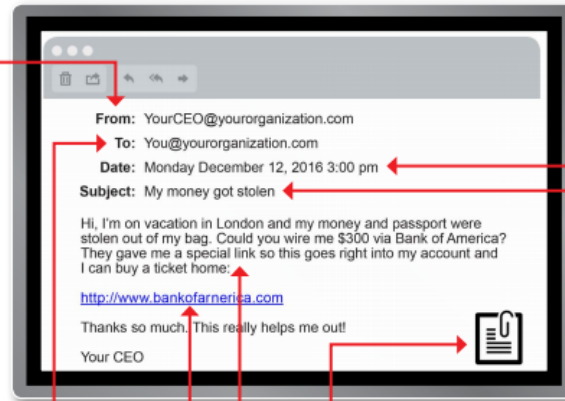
### TO

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.



### HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big red flag**.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, [www.bankofarnerica.com](http://www.bankofarnerica.com) — the “m” is really two characters — “r” and “n.”



### DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?



### SUBJECT

- Did I get an email with a subject line that is **irrelevant or does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?



### ATTACHMENTS

- The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on** is a .txt file.



### CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar or spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd or illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

# Give Them Immediate Feedback Training

- Use Social Engineering Indicators Training



## Oops! You clicked on a phishing email

Please take a minute to review the Social Engineering indicators found in the email you received.  
Hover over the red flags to see details:

To: katieb@knowbe4.com  
From: LinkedIn <linkedin@knowbe4.com>  
Reply-to: LinkedIn <linkedin.bxrye@knowbe4.staging.cyberheist.com>  
Subject: Join my network on LinkedIn

---

**LinkedIn**

Vague explanation of request

**Someone from knowbe4.com has indicated you are a Friend:**

I'd like to add you to my professional network on LinkedIn.

 [View invitation from Someone](#)

---

DID YOU KNOW that LinkedIn can find the answers to your most difficult questions?  
Post those vexing questions on LinkedIn Answers to tap into the knowledge of the world's foremost business experts.

---

**LinkedIn**

This email is not from LinkedIn and the link doesn't take you to the LinkedIn website. Think before you click!

# Keep Training Current

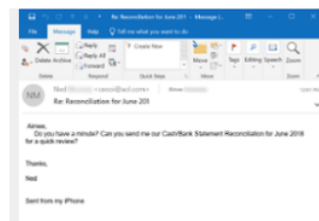
- Scams of the Week



PRODUCTS & SERVICES ▾ FREE TOOLS ▾ PRICING

take reservations?

[Continue Reading](#)



## Scam Of The Week: \*Another\* New CEO Fraud Phishing Wrinkle

Jul 20, 2018 4:08:11 PM By Stu Sjouerman

So, here's a new CEO Fraud phish: see these fresh screen shots from emails reported to us through the free KnowBe4 Phish Alert Button. Bad guys spoof the managing partner and CPA and an ...

[Continue Reading](#)



## [Scam Of The Week] Amazon Prime Day Is Only 4 days away

Jul 12, 2018 4:35:15 PM By Stu Sjouerman

It's a prime opportunity for the bad guys to send a raft of phishing attacks. We do have a "Free Amazon Prime Account" template that we just modified to fit a Prime Day-style scam. It's ...

[Continue Reading](#)



## Scam of The Week: Celebrity Deaths Kate Spade and Anthony Bourdain

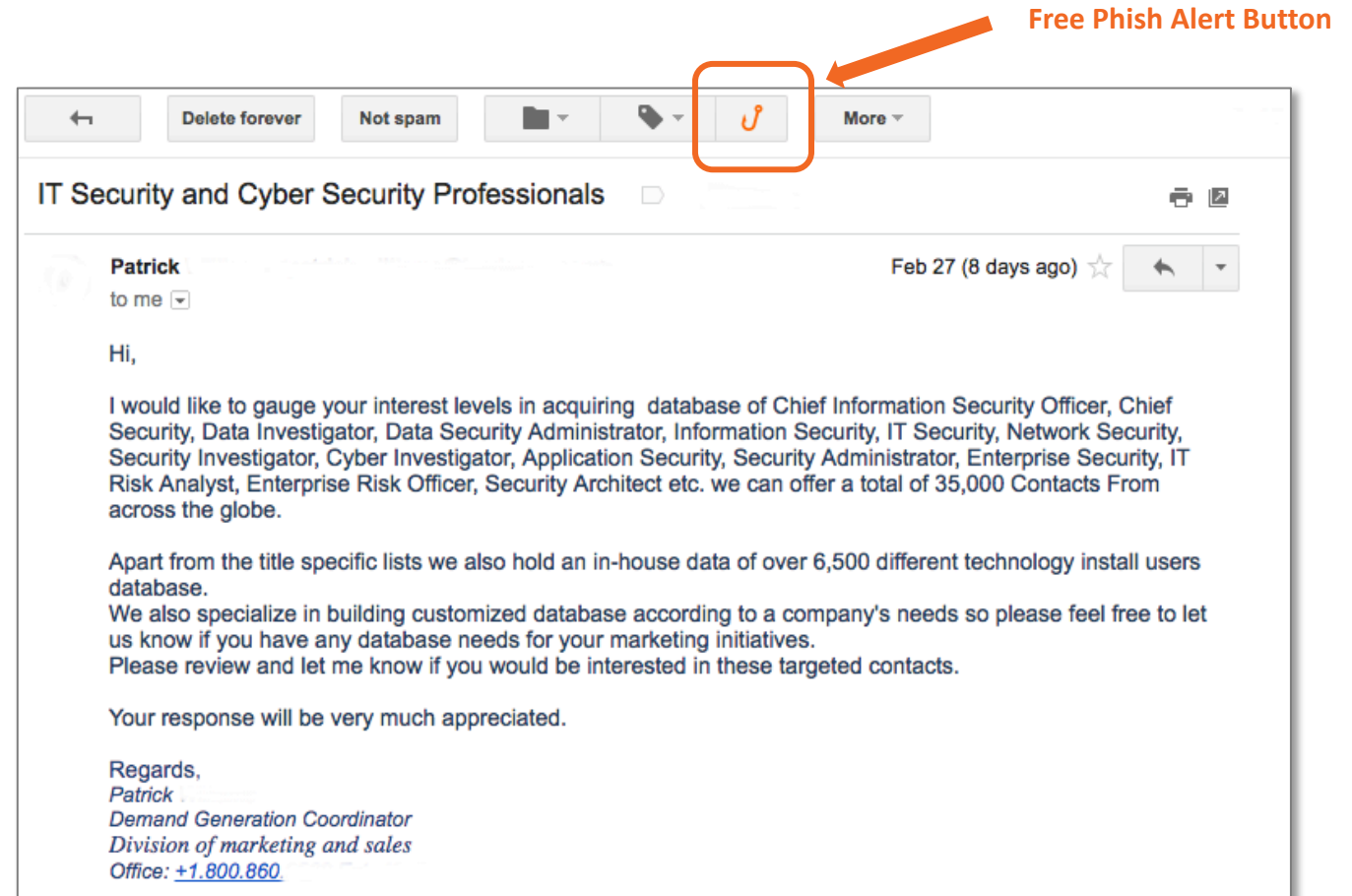
Jun 9, 2018 10:10:56 AM By Stu Sjouerman

Two celebrities committed suicide this week, and unfortunately that's going to be exploited by lowlife internet criminals in a variety of ways.

[Continue Reading](#)

# Give Users A Way To Report Attacks

- Give the users a way to provide the suspect email to someone that can review it
- “Train your employees with regard to phishing, and provide them with a quick and easy way to report suspicious emails.” 2017 DBIR



# Find Out Where the Weaknesses Are

- Get and Use Good Data

Date Range: Last 6 months

Include Selected Campaigns: All Campaigns

Include Campaigns Sent To: All Users

Compare: Failures

Group Comparison By: Location

☐ Include Non-failures

[Submit](#)

Date Range: Last 6 months

Include Selected Campaigns: All Campaigns

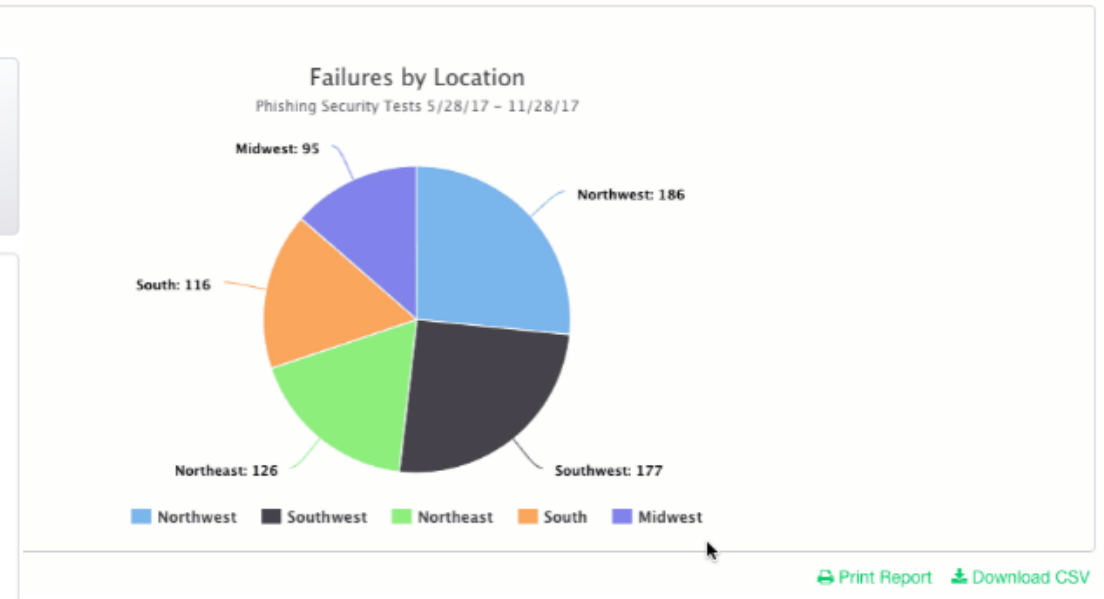
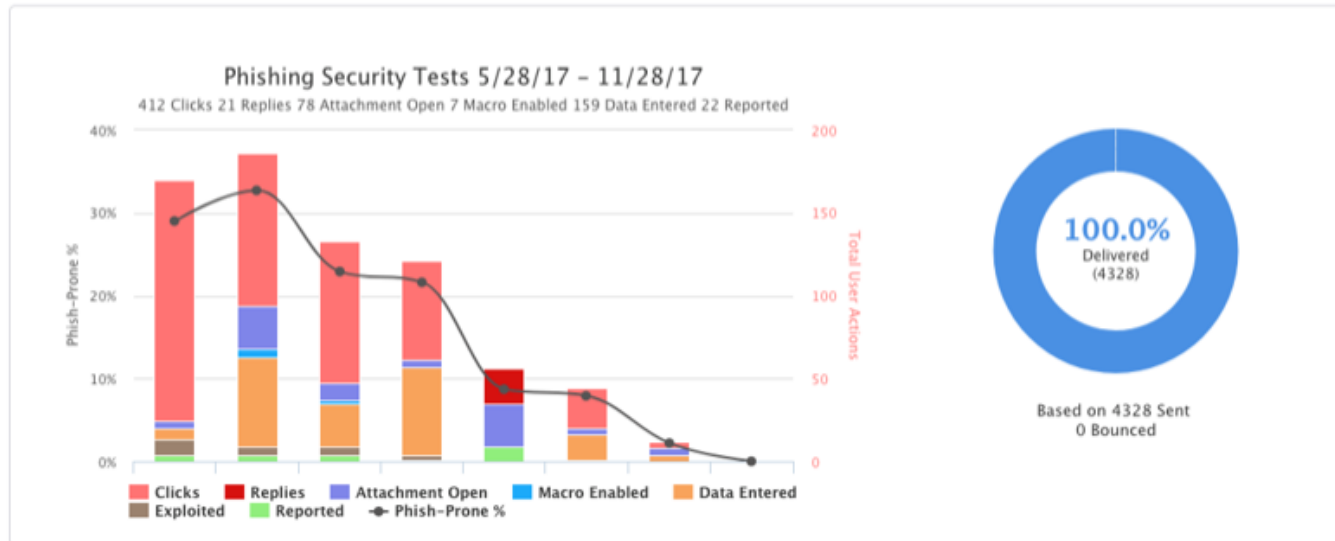
Include Campaigns Sent To: All Users

Compare: Failures

Group Comparison By: -- None --

☐ Include Non-failures

[Submit](#)



# Best Practices

## Training

- Train, test, train
- Testing and training once or twice per year isn't enough
- New employee onboard training (longer and broad)
- Periodic training (shorter and more focused)
- Training on-the-spot (after a failed simulated phishing test)
- Automate as much as possible
- Make a culture where people feel safe reporting security mistakes
  - More carrot and less stick



# Best Practices

- Get senior management approval before conducting any simulated phishing tests
  - Surprises are not good
- Get beginning baseline and ongoing “phish-prone” statistics
- After initial baseline, communicate testing and training strategy to all users
  - It’s a part of the training and changing the culture
- Randomize the phishing times and subjects
  - Avoid sending out every phish test in one big blast
- Do group-, topic-, news-, and season-specific testing mixed in with broad, general categories (e.g. free donuts, etc.)

# Agenda

- Real-Life Hints

# Real-Life Hints

## URL Training

- Help Users Understand How to Read URL Domains to spot the dubious URL links

### Microsoft Office-365

Hello roger\_grimes@infoworld.com  
Sorry, due to a problem with your roger\_grimes@infoworld.com subscription, your email has been suspended.  
If you'd like to continue receiving this message, please click the link below to re-verify your email address.  
Click or tap to follow link.

[RE-VERIFY NOW](#)

This action will take you to the following URL: [https://devopsnw.com/login.microsoftonline.com?userid=roger\\_grimes@infoworld.com](https://devopsnw.com/login.microsoftonline.com?userid=roger_grimes@infoworld.com)

Thanks,  
The Microsoft Office 365 Team

This message was sent from the email address is not monitored. Do not reply to this message.  
[Privacy](#) | [Legal Notices](#)

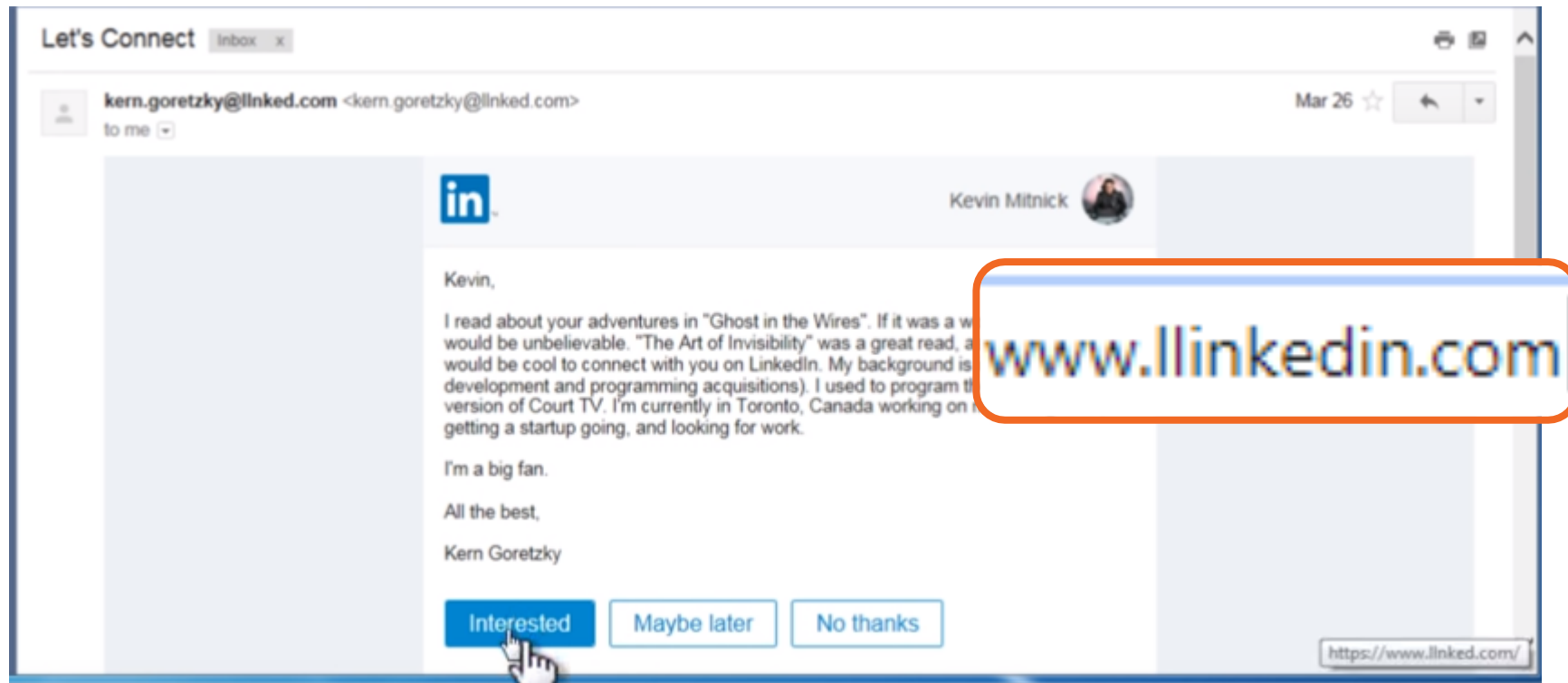
**We hope to continue serving you.**  
**Microsoft Corporation**  
One MSN Way, Redmond, WA 98052

We respect your privacy. Please read our online [Privacy Statement](#).  
This Message was sent from an unmonitored e-mail address. Please do not reply this message.

# Real-Life Hints

## URL Training

- Help Users Understand How to Read URL Domains to spot the dubious URL links



# Real-Life Hints

## Misc

- Good, tested backups
- Require MFA
- Do periodic searches for logon credentials on Internet and darkwebs

# Real-Life Hints

## Honeypots and Red Herrings

- Monitor Internet and darkweb for real account credentials being listed



Password Exposure  
Test



Email Exposure  
Check Pro

[www.knowbe4.com/resources](http://www.knowbe4.com/resources)


# Real-Life Hints


## Honeypots and Red Herrings


- Monitor Internet and darkweb for real account credentials being listed

1 items sorted by Title ▾

F

 Facebook  
roger@banneretcs.com


 **Compromised Login**  
Data stored by this website may have been compromised. Change your password to keep your account safe.

 Facebook  
Personal

username  
roger@banneretcs.com

password  
.....

website  
facebook.com

Good 



# Real-Life Hints

## Misc

- Look for signs email address guessing/harvesting is happening, especially around C-level employees
  - Monitor email server for higher than normal rejections

# Real-Life Hints

## Honeypots and Red Herrings

- Honeypots are great for early warning detection
- Pepper your email server with fake email accounts
  - Monitor internal network for their use
  - Monitor incoming email headed to them
  - Monitor Internet and darkweb for them being listed

# Real-Life Hints

## Misc

- Look for malware signs that may indicate a phishing campaign is coming
  - There are often patterns to malware showing up that point to a coming or successful phishing campaign
  - FBI InfraGard announces signs occasionally

# Resources

## Free IT Security Tools



Domain Doppelgänger



Awareness Program Builder



Domain Spoof Tool



Mailserver Security Assessment



Phish Alert



Ransomware Simulator



Weak Password Test



Phishing Security Test



Second Chance



Email Exposure Check Pro



Training Preview



Breached Password Test



### 12+ Ways to Hack Two-Factor Authentication

All multi-factor authentication (MFA) mechanisms can be compromised, and in some cases, it's as simple as sending a traditional phishing email. Want to know how to defend against MFA hacks? This whitepaper covers over a dozen different ways to hack various types of MFA and how to defend against those attacks.

» Learn More at [www.KnowBe4.com/Resources](http://www.KnowBe4.com/Resources) «

# Questions?

Roger A. Grimes  
Data-Driven Defense Evangelist, KnowBe4

rogerg@knowbe4.com  
Twitter: @rogeragrimes  
<https://www.linkedin.com/in/rogeragrimes/>