



A Master Class on IT Security

Roger Grimes Teaches Phishing Mitigation

Roger A. Grimes
Data-Driven Security Evangelist
rogerg@knowbe4.com



Roger A. Grimes

Data-Driven Defense Evangelist
KnowBe4, Inc.

e: rogerg@knowbe4.com

Twitter: [@RogerAGrimes](https://twitter.com/RogerAGrimes)

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

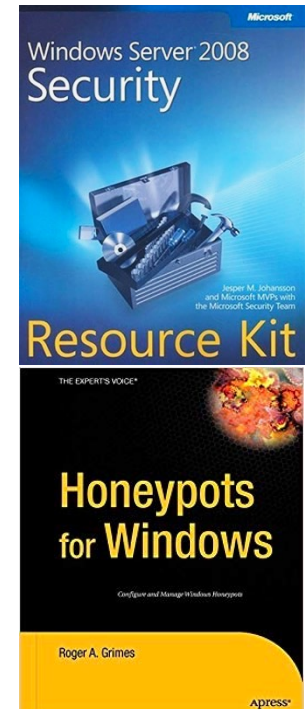
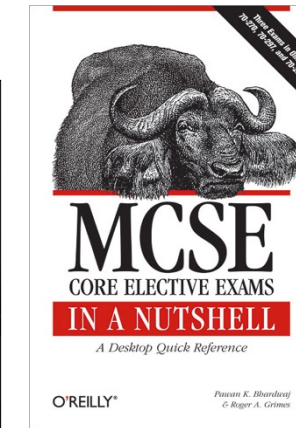
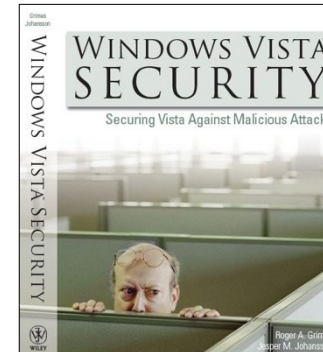
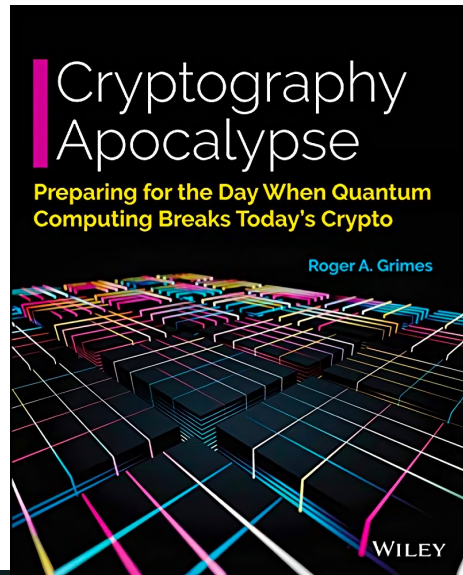
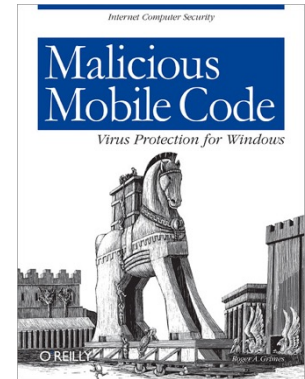
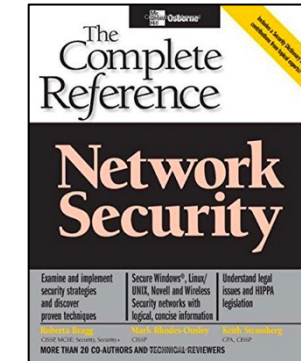
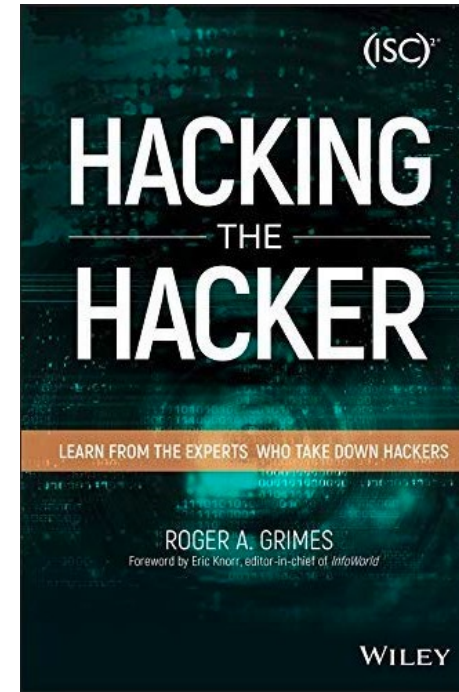
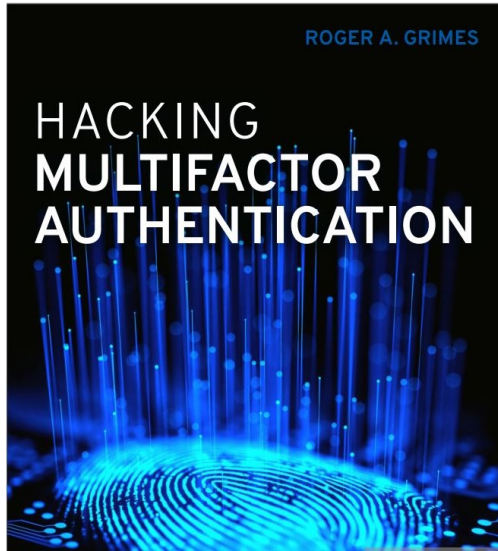
About Roger

- 34 years plus in computer security, 20 years pen testing
- 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 13 books and over 1,300 magazine articles
- *InfoWorld* and *CSO* weekly security columnist 2005 - 2019
- 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



About Us

- The world's largest integrated Security Awareness Training and Simulated Phishing platform
- We help tens of thousands of organizations manage the ongoing problem of social engineering
- CEO & employees are industry veterans in IT Security
- Global Sales, Courseware Development, Customer Success, and Technical Support teams worldwide
- Offices in the USA, UK, Netherlands, Norway, Germany, South Africa, United Arab Emirates, Singapore, Japan, Australia, and Brazil



Today's Presentation

All Things Phishing Mitigation

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

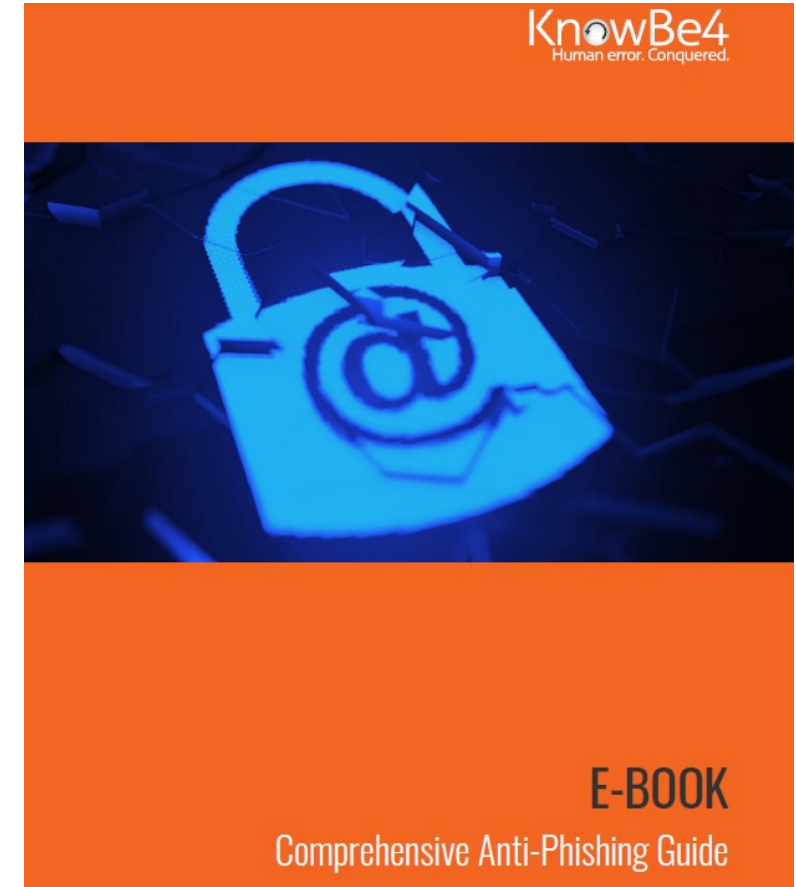
All Anti-Phishing Defenses

Everything You Can Try to Prevent Phishing

- Previous Webinar Version
 - <https://info.knowbe4.com/webinar-stay-out-of-the-net>



- E-book
 - <https://info.knowbe4.com/comprehensive-anti-phishing-guide>

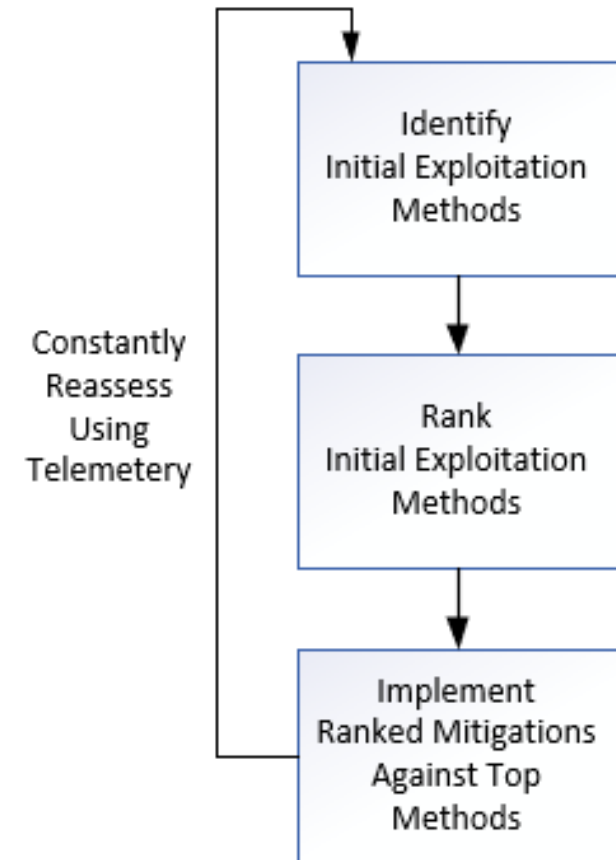


Initial Root Access Exploit Methods

How ALL attackers/malware break in

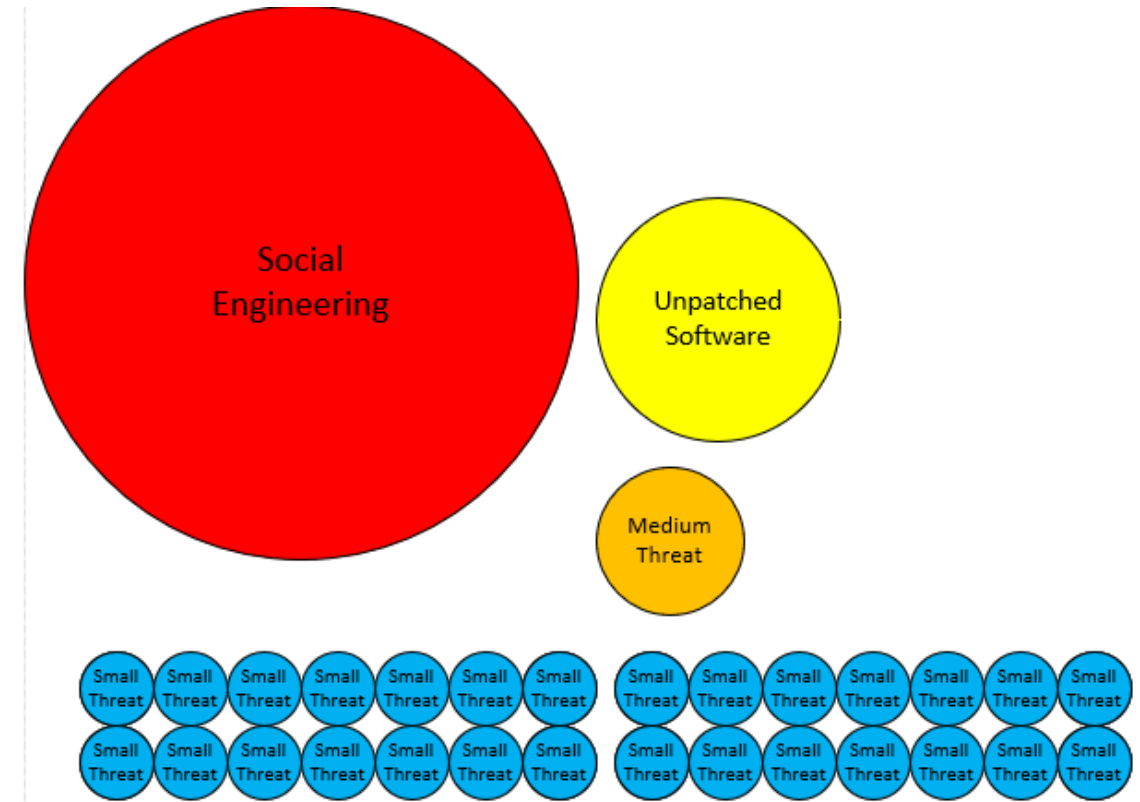
- Social Engineering
- Programming Bug (patch available or not available)
- Authentication Attack
- Malicious Instructions/Scripting
- Data Malformation
- Human Error/Misconfiguration
- Eavesdropping/MitM
- Side Channel/Information Leak
- Brute Force/Computational
- Network Traffic Malformation
- Insider Attack
- 3rd Party Reliance Issue (supply chain/vendor/partner/etc.)
- Physical Attack

Core Data-Driven Defense Principle



Biggest Initial Breach Root Causes for Most Companies

- Social Engineering
- Unpatched Software
- But don't trust me,
measure your own risk



Social engineering is responsible for majority of malicious data breaches

<https://blog.knowbe4.com/phishing-remains-the-most-common-form-of-attack>
<https://info.knowbe4.com/threat-intelligence-to-build-your-data-driven-defense>

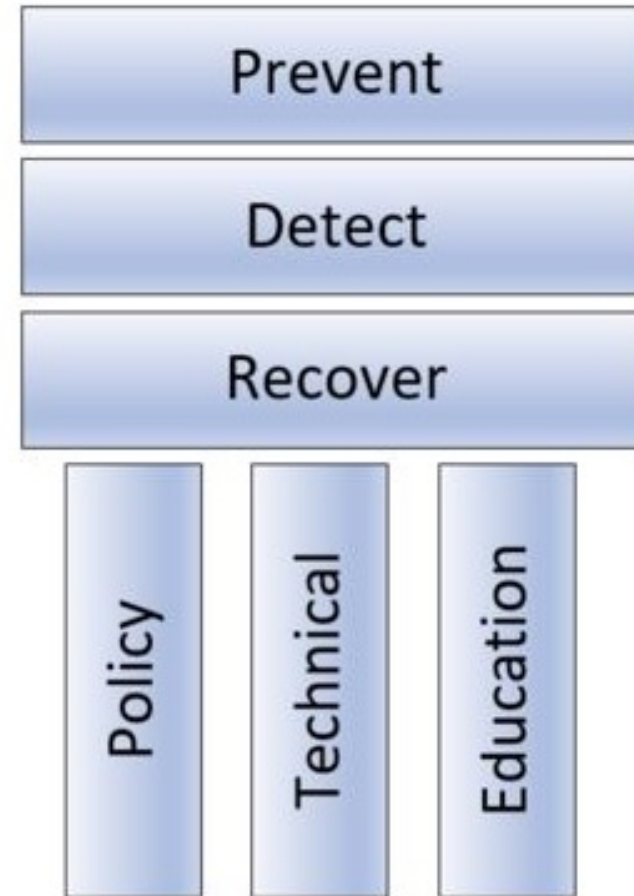
Agenda

- Developing a Comprehensive, Defense-in-Depth Plan

Defending Against Phishing

General Defense Methods

- Policies
- Technical Controls
 - Anti-Malware Software
 - Anti-Spam/Phishing
 - Content Filtering
- Security Awareness Training



<https://blog.knowbe4.com/the-three-pillars-of-the-three-computer-security-pillars>

Defense In Depth Plan

Summary

- Policy and Documentation
- Selection and Implementation of Technical Controls
- Security Awareness Training
- Other Security Checks and Recommendations

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**
- **Consequences** (optional)

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

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

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 maliciously masquerading as a trusted entity to acquire unauthorized information or to created a desired action that is contrary to the victim's or their company's self-interests
- Simply put - a “con”, criminal-intent
- Often done using in-person, email, IM, SMS, phone, etc.
- AKA phishing, spearphishing, 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

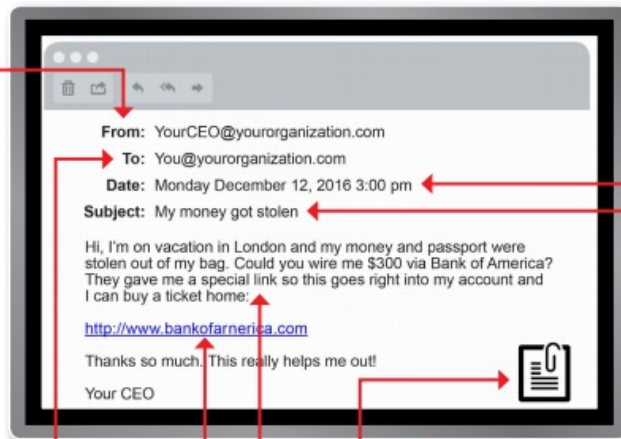
- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner 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 — 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?

<https://blog.knowbe4.com/share-the-red-flags-of-social-engineering-infographic-with-your-employees>

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
- Reduce functionality (locked down desktop)
- 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 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

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, payment instruction changes, etc., **MUST** be confirmed verbally with the legitimate requestor (at least above a certain threshold)

Defense In Depth Plan

Consequences (optional)

To be clear, we believe in more honey and less sticks

Examples:

- More, longer training until failures decrease
- Supervisors give personal counseling, asking employee how team can help them
- Phish-prone rate is reviewed as part of employee's annual review process
- Lockdown Internet access until it can be proven that they can't be as easily phished
- HR actions, up to and including firing

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

- 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
- Free tool from Microsoft that works with a free service from Google
- Can be used to compare all running processes against 70+ antivirus scanners at once on Virus Total (virustotal.com)
- Doesn't slow your system down



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	Virus Total
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
MicrosoftEdge.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	0/68
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

<https://www.csoonline.com/article/2883958/malware/how-to-detect-malware-infection-in-9-easy-steps.html>
<https://www.infoworld.com/article/3014323/security/a-free-almost-foolproof-way-to-check-for-malware.html>

Technical Controls

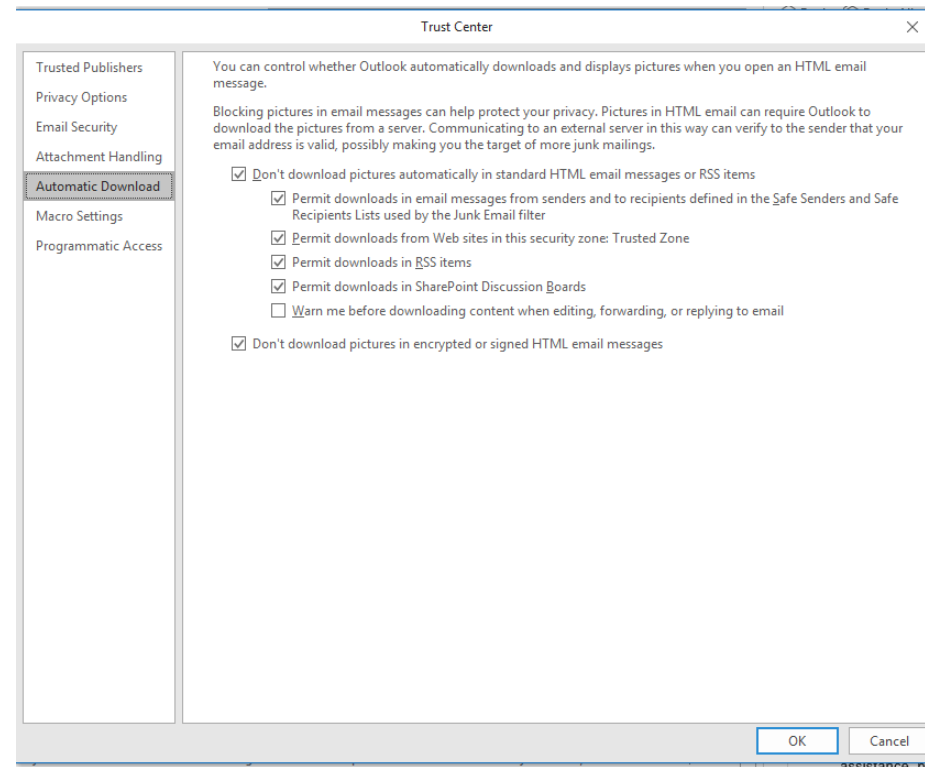
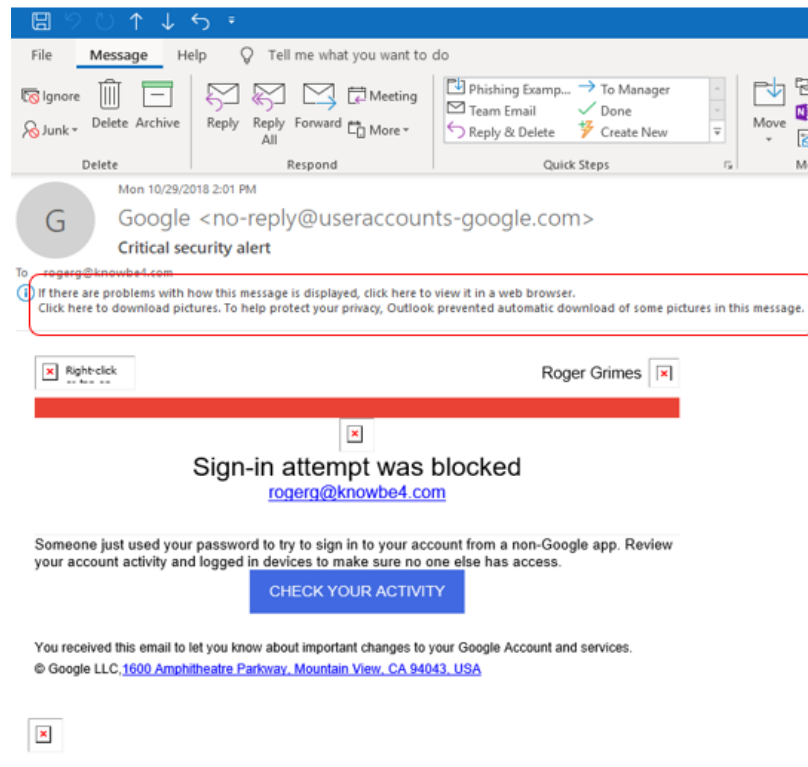
Email-Specific

- Email Client Protections
 - Strongly configured email protections

Technical Controls

Email-Specific

- Email Client Protections



Technical Controls

Email-Client Specific Protections

- Email Client Protections
 - Strongly configure email protections
 - Often enabled by default, don't mess things up
- Browser Protections
- Email Service Provider Protections

Technical Controls

Multi-Factor Authentication (MFA)

Use phishing-resistant MFA whenever you can

- Decreases risk, but not all risk
- I can get around your MFA solution by sending you a simple phishing email
- Doesn't stop malware, business email compromise scams, etc.
- Doesn't work for all sites and services
 - You will still have a password you use in many places, that can be stolen



Technical Controls

Multi-Factor Authentication (MFA)

KnowBe4's Multifactor Authentication web portal

<https://www.knowbe4.com/how-to-hack-multi-factor-authentication>

Free KnowBe4 e-book

41-page Hacking MFA ebook

<https://info.knowbe4.com/12-way-to-hack-two-factor-authentication>

Webinar

12 Ways to Hack MFA webinar

<https://info.knowbe4.com/webinar-12-ways-to-defeat-mfa>

MFA Assessment Tool

Free, Multifactor Authentication Security Assessment tool

<https://www.knowbe4.com/multi-factor-authentication-security-assessment>



Technical Controls

Multi-Factor Authentication (MFA)

Don't Use Easily Phishable MFA and That's Most MFA!

<https://www.linkedin.com/pulse/dont-use-easily-phishable-mfa-thats-most-roger-grimes>



My List of Good, Strong MFA

<https://www.linkedin.com/pulse/my-list-good-strong-mfa-roger-grimes>

Why Is the Majority of Our MFA So Phishable? and US Government Says to Use Phish-Resistant MFA and

<https://www.linkedin.com/pulse/why-majority-our-mfa-so-phishable-roger-grimes> and

<https://blog.knowbe4.com/u.s.-government-says-to-use-phishing-resistant-mfa>

Phishing-Resistant MFA Does Not Mean Un-Phishable

<https://www.linkedin.com/pulse/phishing-resistant-mfa-does-mean-un-phishable-roger-grimes>

Technical Controls

Password Managers

- Allows you to easily use unique, truly random passwords across all sites and services
- Significantly decreases risk of a shared and weak passwords
- But doesn't stop "take action" phishing like business email compromises, running trojans, etc.
- Creates a new single-point-of-failure possibility
 - You should still use one
- Webinar: <https://info.knowbe4.com/truth-about-password-managers>

Technical Controls

Extreme Control: Red/Green Systems

- Every user is given two systems: physical or virtual
 - Business work is done on very locked down system
 - Personal work is done on the other
- Does decrease risk, but not all risk
 - Phishing, ceo fraud emails, etc.
- Nearly doubles operational costs
- Consider one highly secure system instead, Qubes, Application Control app, etc.

Technical Controls

Global Phishing Protection Standards

- **Sender Policy Framework (SPF)**
- **Domain Keys Identified Mail (DKIM)**
- **Domain-based Message Authentication, Reporting and Conformance (DMARC)**
 - **DMARC relies on/uses SPF and DKIM**
- Important point: SPF, DKIM, and DMARC help you protect YOUR domain against spoofing by bad people to others!
- When enabled, receivers can verify whether or not an email that claims to be from your domain is from your domain

SPF & DKIM

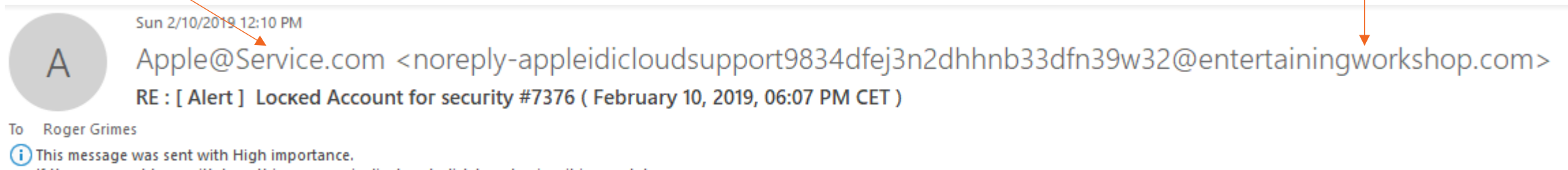
Global Email Authentication Standards

- **Sender Policy Framework (SPF)**
 - Verifies the 5321 **MAIL FROM** domain name address
 - This is the “real” return email address that you may not see

“Friendly From”

Human readable part of “From:” header.

5322.Display
From domain



SPF & DKIM

Global Email Authentication Standards

- **Domain Keys Identified Mail (DKIM)**
 - Uses public/private key pair to adds a digital signature to every outgoing email that links the email to it's sending Internet domain
 - Verified domain is found in the DKIM-Signature header
 - DKIM signatures typically cover most of the email message so that people cannot tamper with content of an email
 - However some of the email headers are NOT included in signature -- specifically headers that tend to be modified as email flows across the Internet (like "Received:" and "Return-Path:" headers).

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;  
d=dmarcian.com; s=s2048g1;  
h=subject:to:cc:references:from:message-id:date:user-agent  
:mime-version:in-reply-to:content-language;  
bh=iVrm4GcK3W8w6dNUvDCTJY22HJmChvuZ7JCebDsft0g=;  
b=CVIqiyEdtNmyv18PAbimb87xBL15wQPS2k89oEg14uz4LugQLf3U/Vw7GpRLciiR0+  
dCpszAlw0WNWBGcRmJKM/dzLwTR6wTth/vwkXpcf8tT2/K9c1Le649YRnwtDnwmNwpXu  
PEqzATj0uj6hiEUmy4UL1/e6tP58Gb5UMCKpsXdV1+J3Qu3Jech7k5250LQRLqsVetAE  
G7fCQ6GFpaAApnRXa2BT0k7gHPB4Ak8BYy7iINT2ckuPi7ETuCaA4bqp1Kpm5LlpsTKUW  
x/gAsB94w5fv5Q+UTZhis3LTEz1Ymh5UEi8Ix+02mUMTBXgINpmxV9MqdF0AhVyC1uef  
NTHw==
```

DMARC

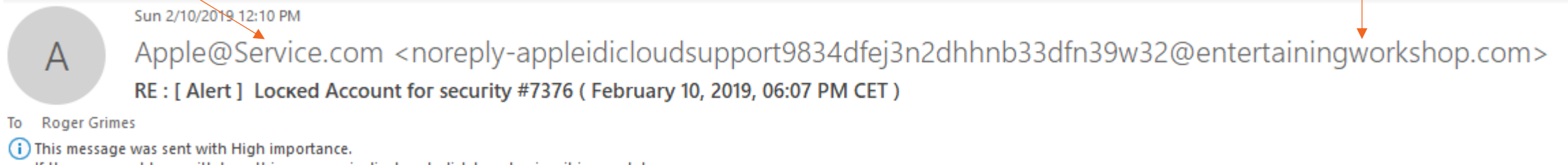
Global Email Authentication Standards

- **Domain-based Message Authentication, Reporting and Conformance (DMARC)**
 - Helps to tell receivers how to treat emails that fail SPF and/or DKIM
 - DMARC requires the domains that SPF and DKIM verifies to match what is found in the 5322.From address
 - Helps senders with diagnostic reports

“Friendly From”

Human readable part of “From:” header.

5322.Display
From domain

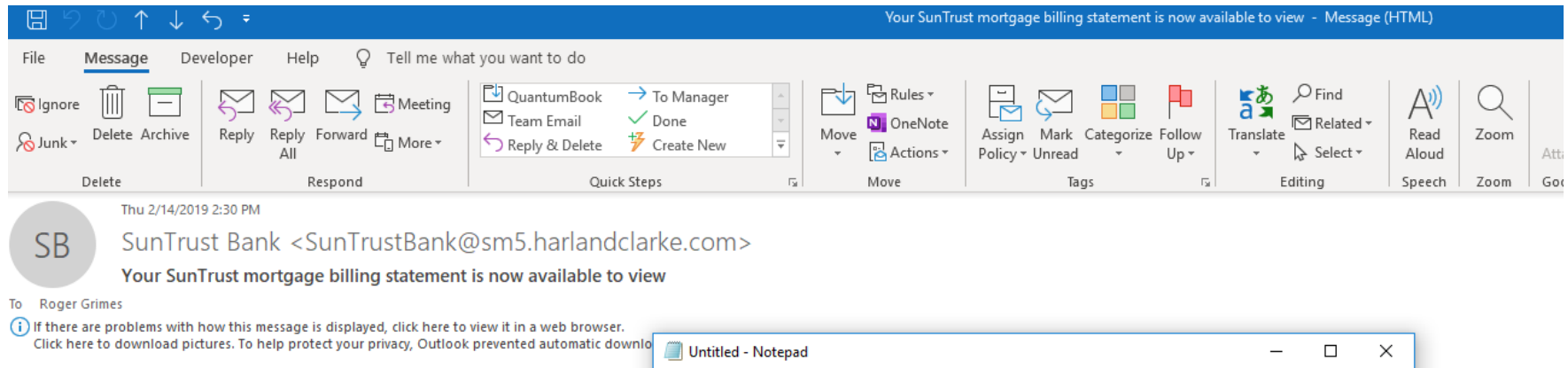


Technical Controls

Global Phishing Protection Standards

- Both sides need to implement in order to be effective
- All work using TXT DNS records configured by sender, which is sent along with each email by enabled email service
- All work by receivers then using enabled email service to verify when receiving email
- You need to implement

Technical Controls



Pass = Verified Domain

3. Select Mortgage Loan from the My Accounts list
4. Click Statements and Documents

It is our job to stay connected with you and learn more about your financial goals. Let us know how we can help. We are just a [click](#) away or call us today at 800.634.7928, Monday through Friday from 8 a.m. to 8 p.m., and 9 a.m. to 3 p.m. ET, on Saturday.

Technical Controls

The screenshot shows an Outlook email window with the following details:

- Sender:** Microsoftline <v5pz@onmicrosoft.com>
- Ticket #:** 5711310
- To:** roger_grimes@infoworld.com
- Subject:** Your request (14299790) has been updated. To add additional comments...
- Body:** Hello, Good day! Thank you for contacting Microsoft Commercial Billing. My name is Jerica, the Support Ambassador whom you spoke with. As discussed, you called us today to change your credit card information. We expect that the new card will be the charge in the next billing cycle. For future reference kindly click the link below. Add, update, or remove credit card or bank account - <https://portal.office.com/Support/AltUS>. It has been a pleasure working with you. If you need assistance in the future, you may call us or create a new support request. Upon closing this billing case, a short survey with 5-star being great will appear in the Support Tickets page in your Office 365 Admin portal (<https://portal.office.com/Support/AltUS>). Thank you for choosing Microsoft.

The Notepad window displays the following SMTP headers:

```
Authentication-Results-Original: spf=fail (sender IP is 80.255.3.116)
smtp.mailfrom=august-debouzy.com; infoworld.com; dkim=none (message not signed) header.d=none;infoworld.com; dmarc=none action=none
header.from=onmicrosoft.com;
Received-SPF: Fail (protection.outlook.com: domain of august-debouzy.com does not designate 80.255.3.116 as permitted sender)
receiver=protection.outlook.com; client-ip=80.255.3.116; helo=fatafit.com;
Received: from fatafit.com (80.255.3.116) by
VE1EUR02FT030.mail.protection.outlook.com (10.152.12.127) with Microsoft SMTP
Server (version=TLS1_0, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA) id
15.20.1900.16 via Frontend Transport; Sat, 18 May 2019 00:36:52 +0000
Received: from (helo=abmas01.marketo.org) by abmta15.marketo.org
(envelope-from <info@heritage.org>) (ecelerity 4.2.38.62370 r(:)) with
ESMTP id B1/35-06954-6704FDC5; Fri, 17 May 2019 18:15:02 -0500
From: Microsoftline <v5pz@onmicrosoft.com>
To: <roger_grimes@infoworld.com>
```

A red box highlights the "Received-SPF: Fail" line, and a red arrow points from it to a red text box below.

Fail = Bad or Unverified Domain

Technical Controls

Domain Keys Identified Mail (DKIM)

- Designed to prevent sender email address domain spoofing by receiver verifying the digital signature of the mail server domain sent with each email
- Checks for domain spoofing in 5322 Display Name field
- 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 Verification Results

```
Received: from C01NAM05FT032.eop-nam05.prod.protection.outlook.com  
(2a01:111:f400:7e50::207) by C02PR04CA0151.outlook.office365.com  
(2603:10b6:104::29) with Microsoft SMTP Server (version=TLS1_2,  
cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384) id 15.20.1622.16 via Frontend  
Transport; Thu, 14 Feb 2019 19:31:58 +0000  
Authentication-Results: spf=pass (sender IP is 63.240.155.138)  
smtp.mailfrom=sm5.harlandclarke.com; banneretcs.com; dkim=pass (signature was  
verified) header.d=sm5.harlandclarke.com;banneretcs.com; dmarc=bestguesspass  
action=none header.from=sm5.harlandclarke.com;compauth=pass reason=109
```

Technical Controls

DMARC

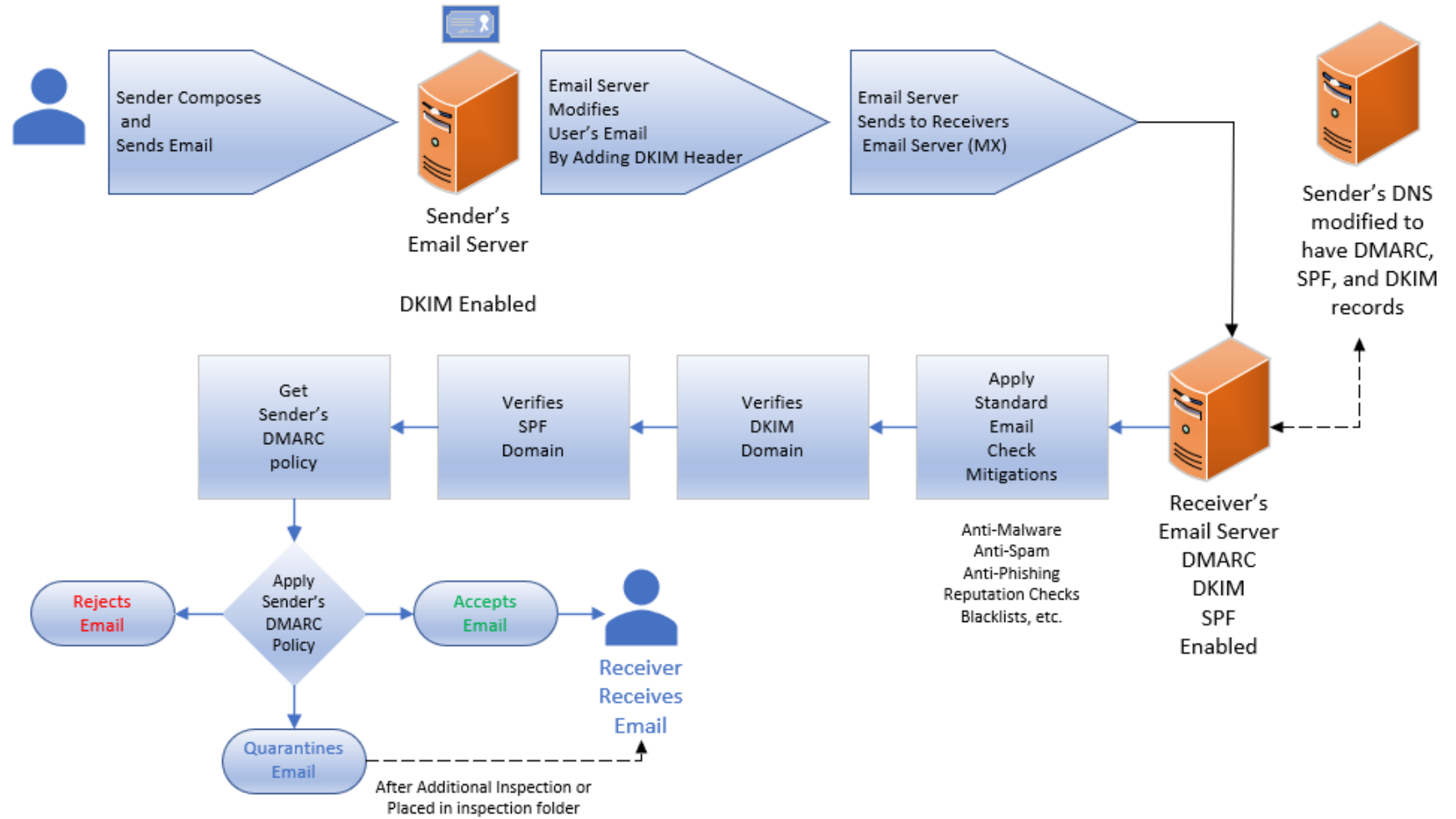
- Sender can indicate whether they use SPF and/or DKIM, which the receiver can verify and rely on, and how a receiver should treat failed messages
- TXT IN "v=DMARC1;p=quarantine;pct=100;rua=mailto:dmarccheck@example.com;"

P =

- None – Take no special treatment for failed emails
- Quarantine – Treat as suspicious
- Reject – Reject email at server before it gets to client

SPF, DKIM, and DMARC

Putting it all together



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 (hackers can register their domains), but they do help (prevent spoofing of other people's domains)
- You should implement
- Be careful 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`
 - Get more detail here:
<https://www.csoonline.com/article/3333916/windows-security/i-can-get-and-crack-your-password-hashes-from-email.html>

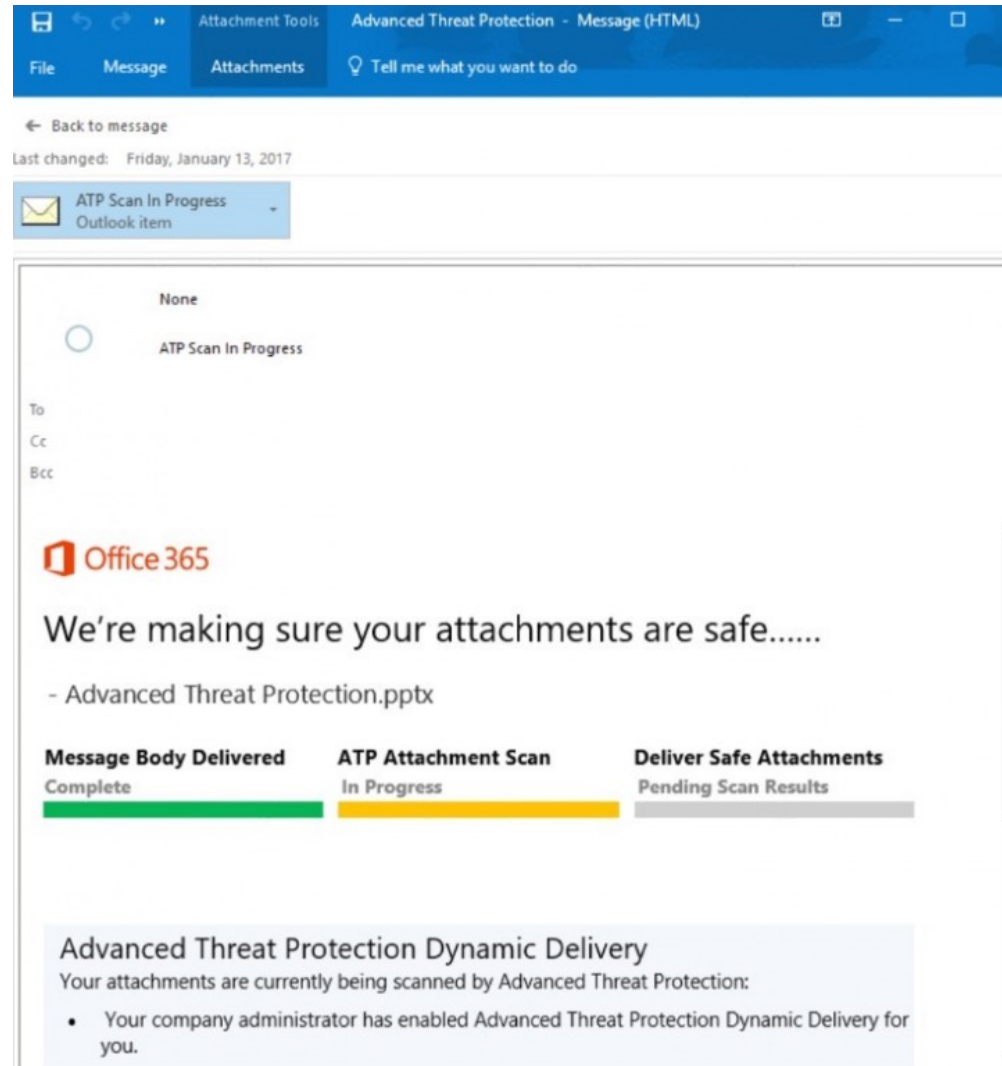
Technical Controls

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



The screenshot shows an Outlook interface with a message titled "Advanced Threat Protection - Message (HTML)". The message content includes:

- Back to message
- Last changed: Friday, January 13, 2017
- ATP Scan In Progress Outlook item
- None
- ATP Scan In Progress
- To
- Cc
- Bcc
- Office 365 logo
- We're making sure your attachments are safe.....
- Advanced Threat Protection.pptx
- Progress indicators:
 - Message Body Delivered: Complete (green bar)
 - ATP Attachment Scan: In Progress (yellow bar)
 - Deliver Safe Attachments: Pending Scan Results (grey bar)
- Advanced Threat Protection Dynamic Delivery section:
 - Your attachments are currently being scanned by Advanced Threat Protection:
 - Your company administrator has enabled Advanced Threat Protection Dynamic Delivery for you.

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

DNS Checks

- You can have email arriving from suspicious domains rejected or further inspected
- DNS domains that were created within the last 24-hours
 - Very, very likely to be a rogue domain
- Can be implemented in DNS, email server product, or email protection product

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

KnowBe4 Security Awareness Training



Baseline Testing

We provide baseline testing to assess the Phish-Prone™ percentage of your users through a free simulated phishing attack.



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, thousands 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!

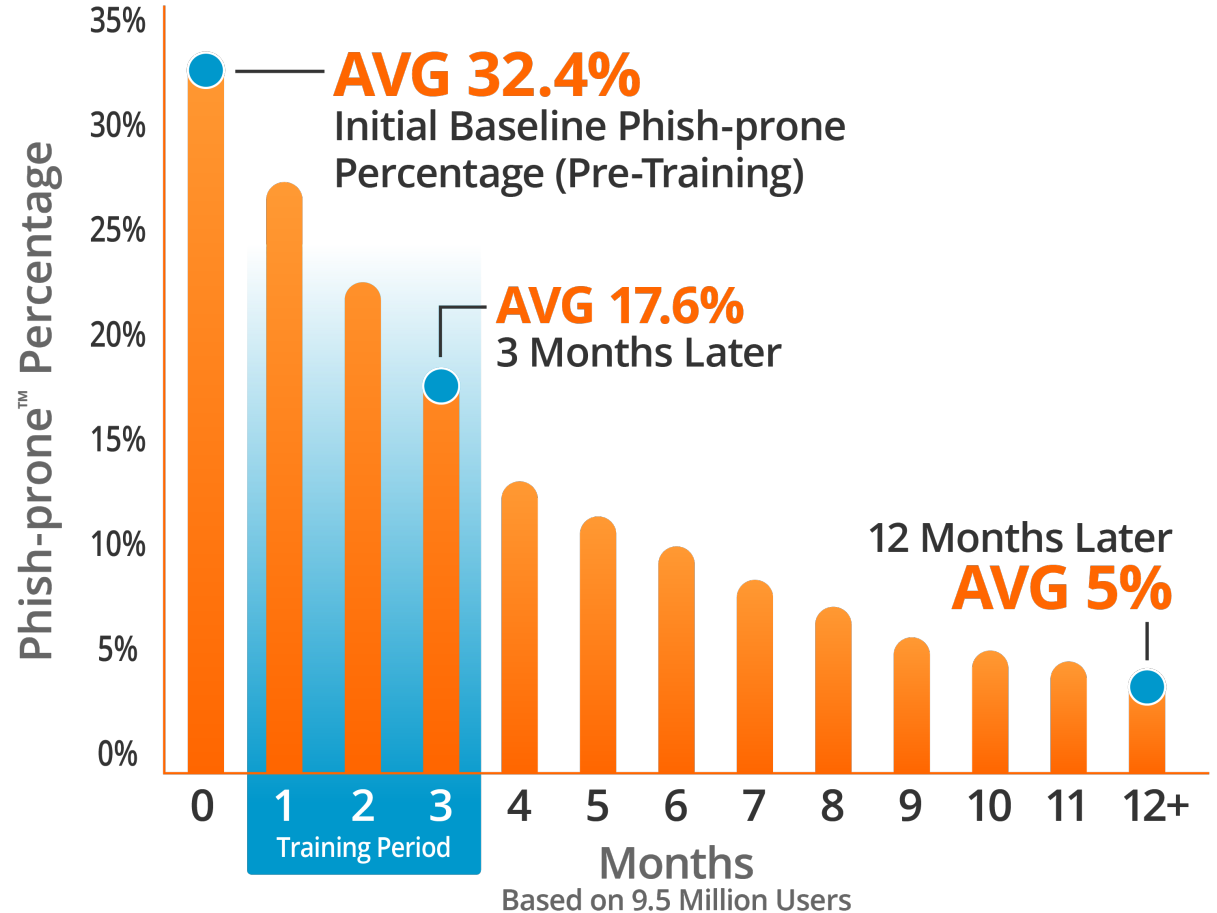


Generating Industry-Leading Results and ROI

- Reduced Malware and Ransomware Infections
- Reduced Data Loss
- Reduced Potential Cyber-theft
- Increased User Productivity
- Users Have Security Top of Mind

85% Average Improvement

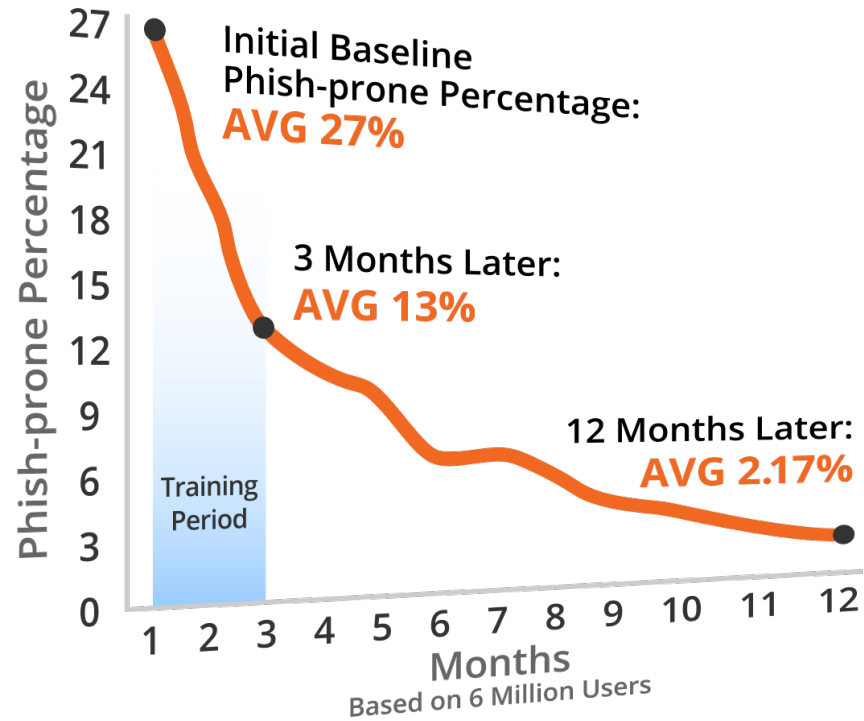
Across all industries and sizes from baseline testing to one year or more of ongoing training and testing



Source: 2022 KnowBe4 Phishing by Industry Benchmarking Report

Note: The initial Phish-prone Percentage is calculated on the basis of all users evaluated. These users had not received any training with the KnowBe4 console prior to the evaluation. Subsequent time periods reflect Phish-prone Percentages for the subset of users who received training with the KnowBe4 console.

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

Train Like You're Marketing

- Frequent
- Redundant
- Entertaining

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, Seasons, 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

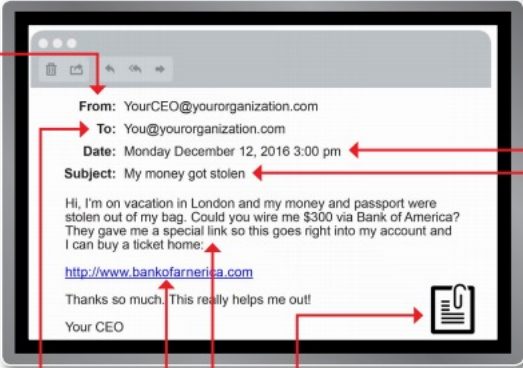
Spear Phish Your Employees

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 micorsolt-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 — 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?

<https://blog.knowbe4.com/share-the-red-flags-of-social-engineering-infographic-with-your-employees>

Give Them Immediate Feedback Training

- Use Social Engineering Indicators Training

KnowBe4
Human error. Conquered.

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

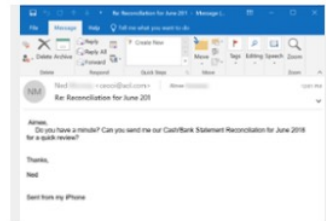
- Scams of the Week



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 Sjouwerman

So, here's a new CEO Fraud phishing: 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 Sjouwerman

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

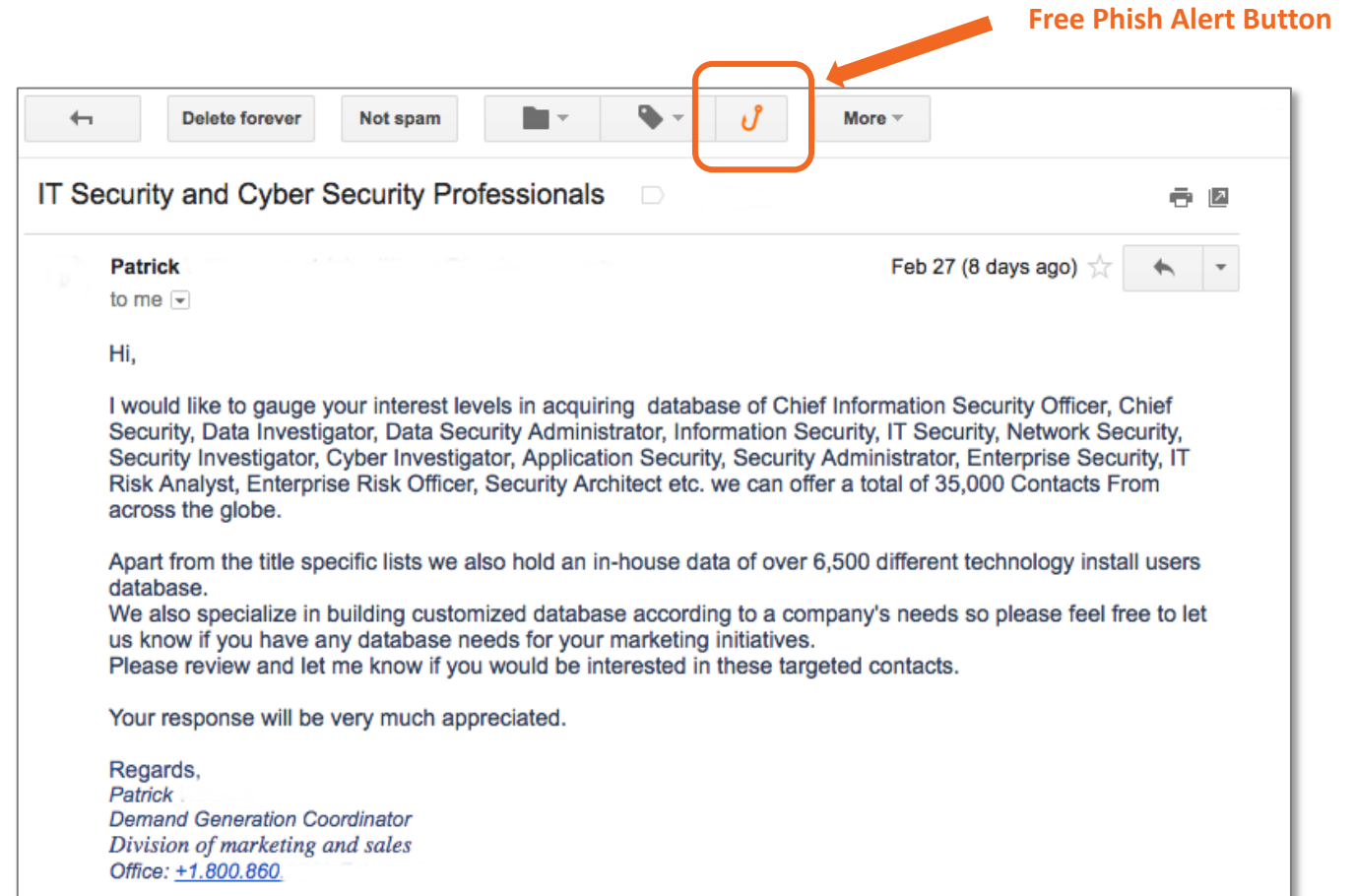
📅 Jun 9, 2018 10:10:56 AM 👤 By Stu Sjouwerman

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

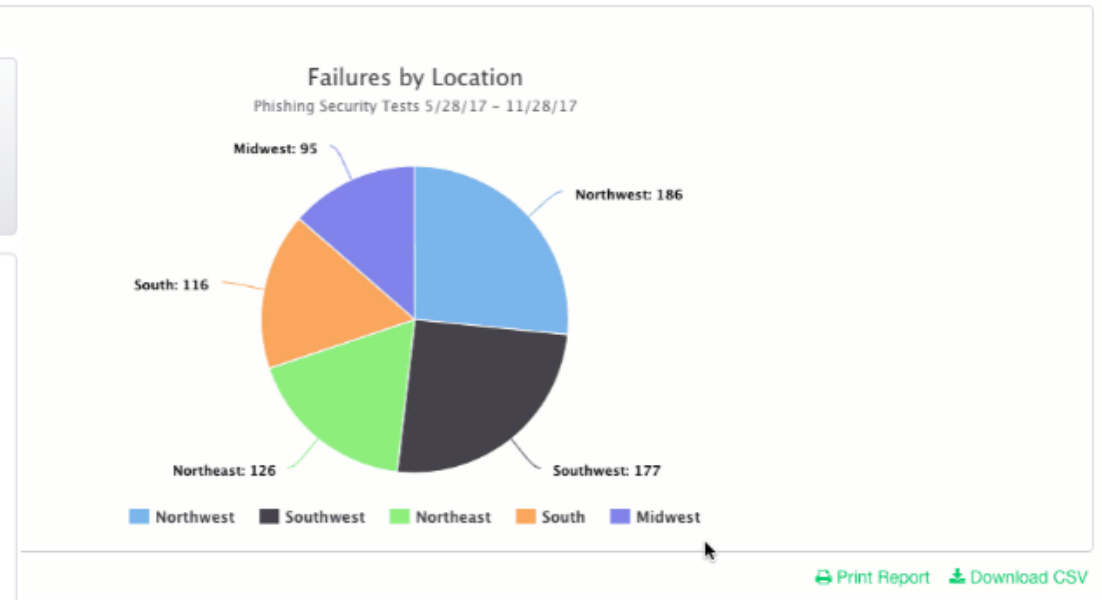
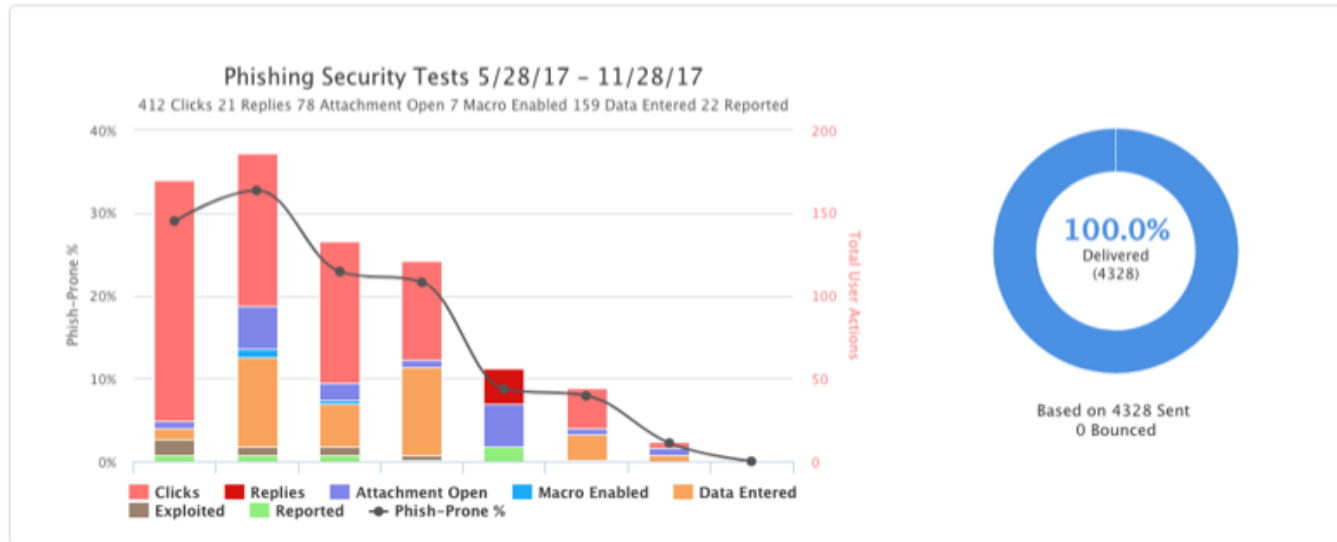


Find Out Where the Weaknesses Are

- 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

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 reactivate your account, please visit https://devopsnw.com/login.microsoftonline.com?userid=roger_grimes@infoworld.com without interruption. kindly re-verify now.

RE-VERIFY

 https://devopsnw.com/login.microsoftonline.com?userid=roger_grimes@infoworld.com

This action

Thanks,
The Microsoft Office

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

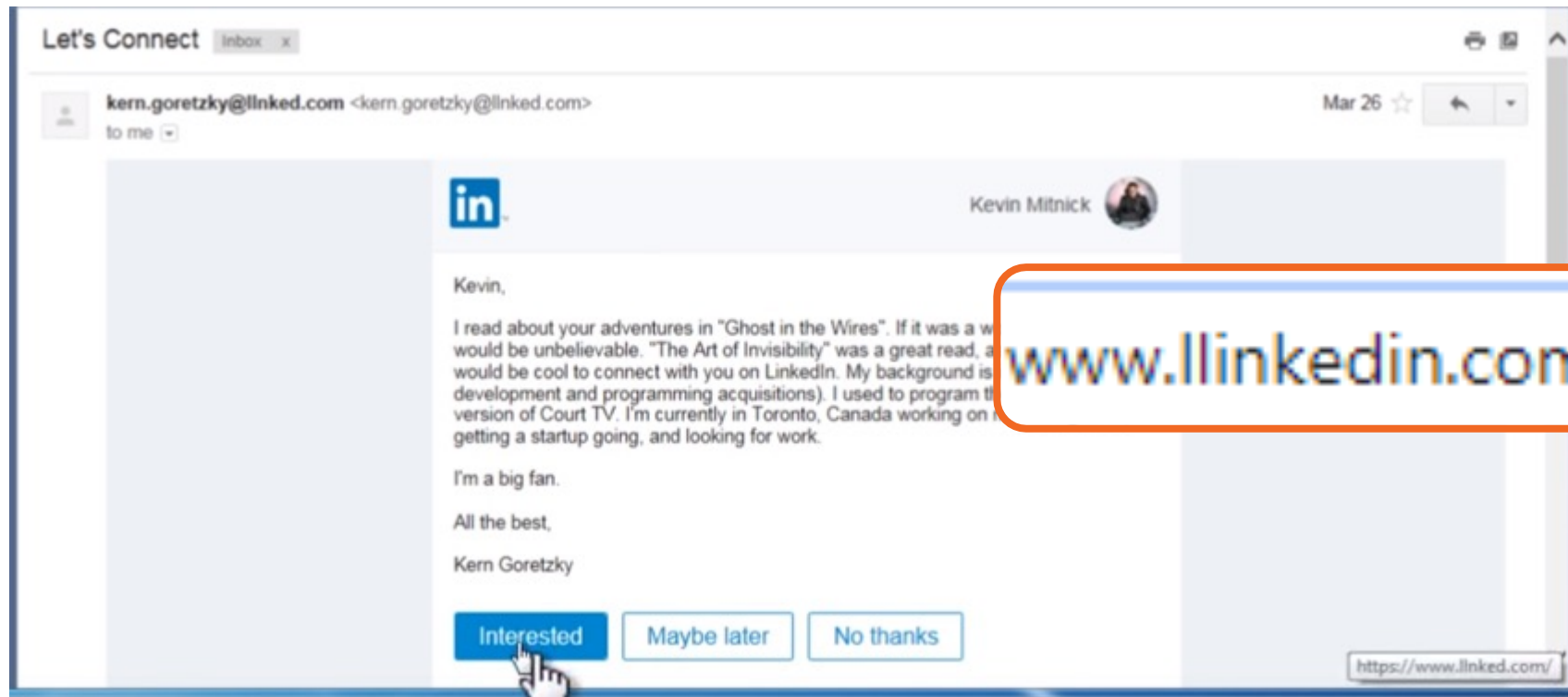
We hope to continue serving you.
Microsoft Corporation
One MSN Way, Redmond, WA 98052

We respects 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

URL Training

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

Bank of America Alert: Unlock Your Account Important Message From Bank Of America®



Bank of America <BankofAmerica@customerloyalty.accounts.com>(Bank of America via shakawaaye.com)
To Roger Grimes

Update Your Powered By office 365



Office 365 <no-reply1@soft.com>(Office 365 via ds01099.snspreview7.com.au)
To Roger Grimes

Your Shipping Documents.




MAERSK <info@onlinealxex.com.pl>(MAERSK via idg.onmicrosoft.com)
To roger_grimes@infoworld.com

Ticket #: 5711310



Microsoftonline <v5pz@onmicrosoft.com>
To roger_grimes@infoworld.com

 If there are problems with how this message is displayed, click here to view it in a web browser.



THE RED FLAGS OF ROGUE URLs

Spotting malicious URLs is a bit of an art. The examples represented here are some of the common tricks used by hackers and phishers to fool users into visiting malicious websites. The methods shown here could be used by legitimate services, but if you see one of these "tricks" you need to make sure you're dealing with the organization you think you are.

Look-a-Like Domains

Domain names which **seem** to belong to respected, trusted brands.

Slight Misspellings

 Microsoftonline
<v5pz@onmicrosoft.com>

 www.llnkedin.com

Brand name in URL, but not real brand domain

 ee.microsoft.co.login-update-dec20.info

 www.paypal.com.bank/logon?user=johnsmith@gmail.com

 ww17.googlechromeupdates.com/

Brand name in email address but doesn't match brand domain

 Bank of America
<BankofAmerica@customerloyalty.accounts.com>

Brand name is in URL but not part of the domain name

 devopsnw.com/login.microsoftonline.com?userid=johnsmith

URL Domain Name Encoding

 <https://%77%77%77%6B%6E%6F%77%62%65%63%6F%6D>

Shortened URLs

When clicking on a **shortened URL**, watch out for malicious redirection.

 <https://bit.ly/2SnA7Fnm>

Domain Mismatches

 Human Services .gov
<Despina.Orrantia6731610@gmx.com>

 <https://www.le-blog-qui-assure.com/>

Strange Originating Domains

 MAERSK
<info@onlinealxex.com.pl>

Overly Long URLs

URLs with 100 or more characters in order to **obscure the true domain**.

 <http://innocentwebsite.com/irs.gov/logon/fasdjkg-sajdkjndfjnbkasldjfbkajsdbfkbjbasdf/adsnfjksdngkfdgfgjhgfd/ght.php>

File Attachment is an Image/Link

It looks like a file attachment, but is really an **image file with a malicious URL**.

 INV39391.pdf
52 KB  <https://d.pr/free/f/jsaec>
Click or tap to follow link.

Open Redirectors

URLs which have hidden links to completely different web sites at the end.

 t-info.mail.adobe.com/r/?id=hc347a&p1=evilwebsite.com

KnowBe4

<https://blog.knowbe4.com/top-12-most-common-rogue-url-tricks>

Real-Life Hints

Misc

Training

- Give kudos for catching phishes

From: InfoSec Team <infosec@example.com>
Sent: Wednesday, September 16, 2020 8:50 AM
Subject: Your PAB Report Update (NAPL)

Roger,

Thank you for your recent phish-alert button report.

Upon investigation, we have verified that the email you reported was a *real phishing attempt*.

Because of users like you, we are able to identify and respond to threats like these, quickly and safely, to ensure the best security for everyone here at KnowBe4.

Your cooperation and resilience keeps our "human firewall" incredibly strong and sets an example for others to follow.

WELL DONE! KEEP IT UP!

Sincerely,

The Example InfoSec Team

(NOTE: This is an automated email)

Real-Life Hints

Misc

- Make people who do the right thing “heroes”, use them as examples
- “Gold star” “official” certificates for people who complete training and don’t get phished when tested
- Personalize the Why – i.e. “We will teach you and your family how to be safer at home with your own information and ours.”
- Cybersafety sign – X number of days since successful phish signs
- Look for signs email address guessing/harvesting is happening, especially around C-level employees
 - Monitor email server for higher than normal rejections

Questions?

Roger A. Grimes
Data-Driven Defense Evangelist, KnowBe4

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