Fighting Back Against Business Email Compromise Attacks

Presented by The Hartford and KnowBe4

Daniel Silverman - Underwriting Director, Specialized CyberTech Risks, Global Specialty - The Hartford
Keith Tagliaferri - Director, Cyber Claim Practices - The Hartford
Roger A. Grimes - Data-Driven Security Evangelist - KnowBe4

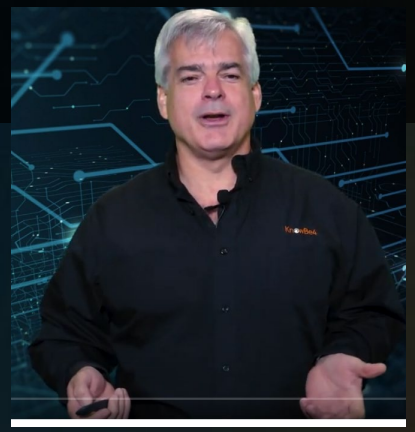
June 27, 2024

The Hartford

BEC Scams

Identifying and Preventing Business Email Compromise Attacks

KnowBe4
Human error. Conquered.



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
LinkedIn: https://www.linkedin.com/in/rogeragrimes/
Mastodon: https://infosec.exchange/@rogeragrimes
Bluesky: rogeragrimes@bsky.social

About Roger

- 35 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 14 books and over 1,400 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:

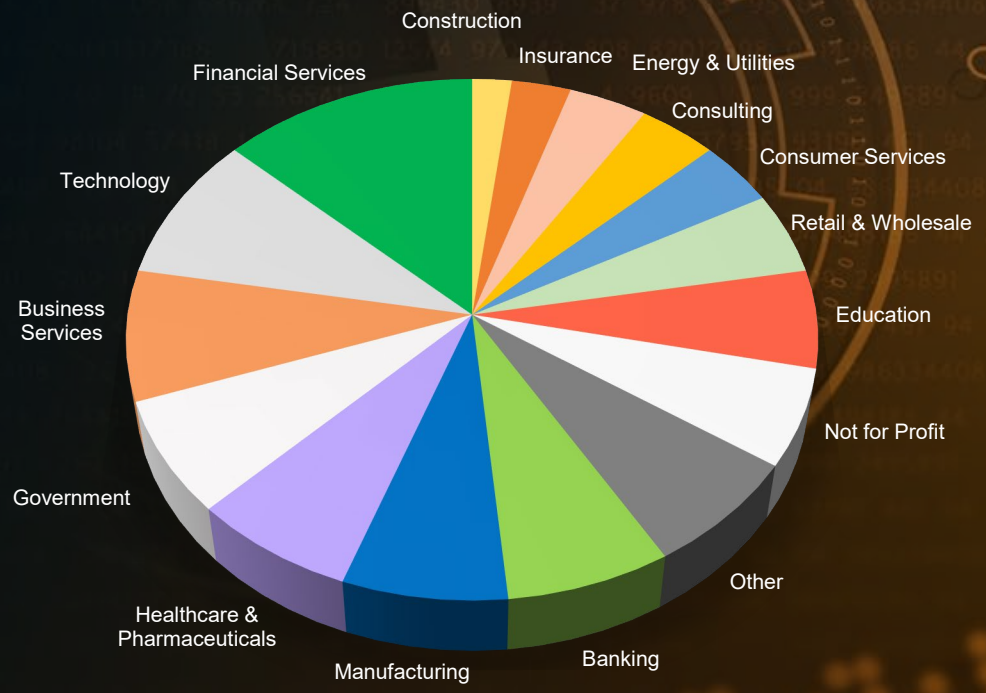
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

Roger's Books

Over

60,000

Customers



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, India, Germany, South Africa, United Arab Emirates, Singapore, Japan, Australia, and Brazil

FORRESTER®
WAVE LEADER 2022
Security Awareness And Training Solutions

AMERICA'S FASTEST-GROWING PRIVATE COMPANIES
Inc. 500

Gartner peerinsights customers' choice 2021™

KnowBe4
Human error. Conquered.

Agenda

- Intro to BEC Scams
- Examples of BEC Scams
- Defenses

Agenda

- Intro to BEC Scams
- Examples of BEC Scams
- Defenses

BEC Scams

Definitions

Business Email Compromise scam

- A social engineering scam in which cybercriminals spoof a company or someone and trick the victim into executing unauthorized money transfers or transfers of confidential information
- FBI says “It’s a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.”

- In short, phishing often involving money transfers
- Often targets Accounting, Accounts Payable, Finance, HR, Executive team, IT, Real Estate officials

Spear Phishing

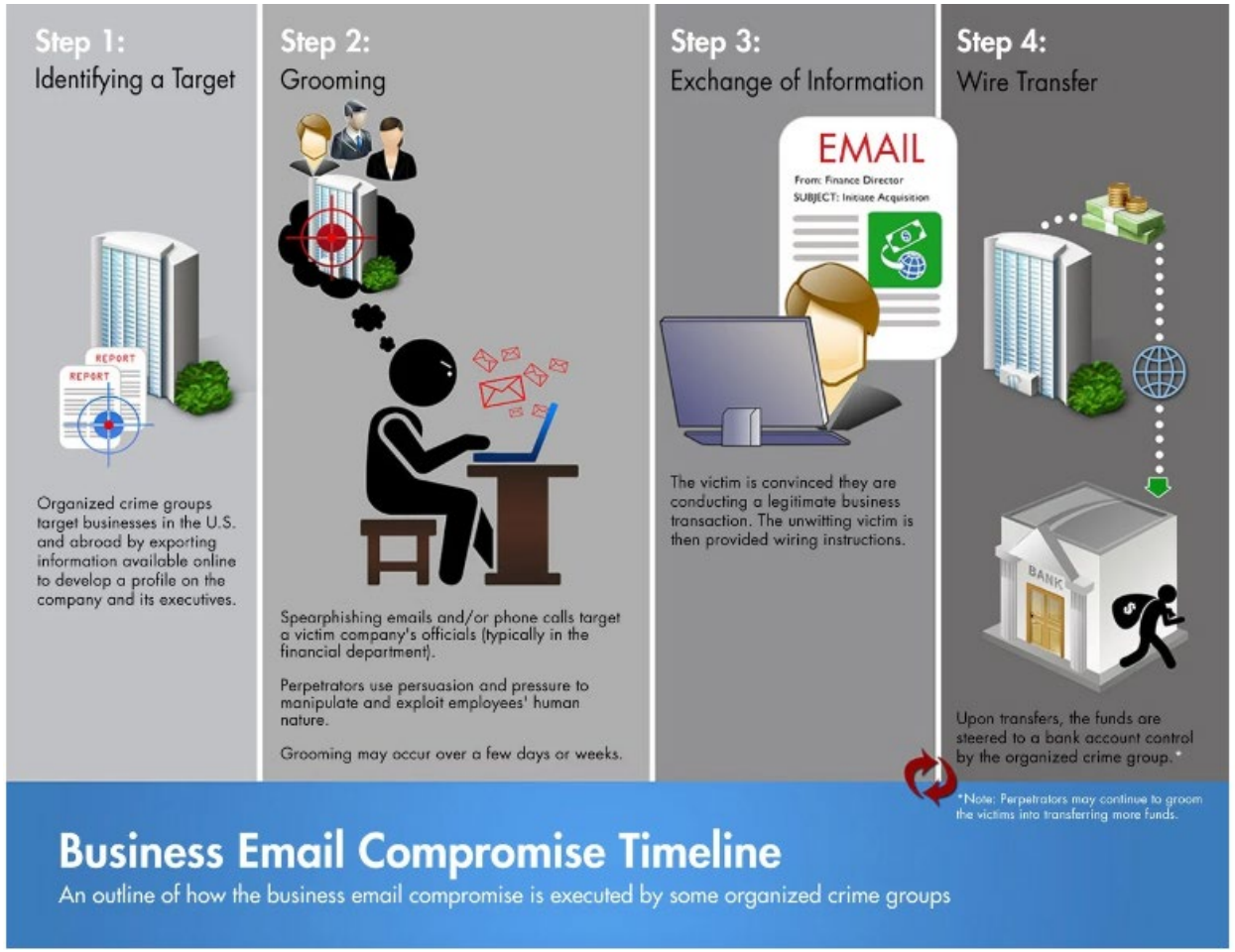
Definition

- Spear phishing is phishing targeted to a particular person or group often with some non-public knowledge used in the phishing attack
- BEC scams are often spear phishing scams
- Barracuda Networks says although spear phishing made up less than 0.1% of attempted email attacks…

…it accounted for over 66% of successful breaches

https://blog.knowbe4.com/spear-phishing-trends-2023
https://www.linkedin.com/pulse/you-need-focus-more-preventing-spear-phishing-attacks-roger-grimes/

BEC Scams



https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/business-email-compromise

BEC Scams

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

June 9, 2023

Alert Number
I-060923-PSA

Business Email Compromise: The $50 Billion Scam

This Public Service Announcement is an update and companion piece to

- After ransomware, BEC scams cost victims the most damage
- FBI says BEC scams have cost victims over $50B
- https://www.ic3.gov/Media/Y2023/PSA230609

BEC Real Estate Scams

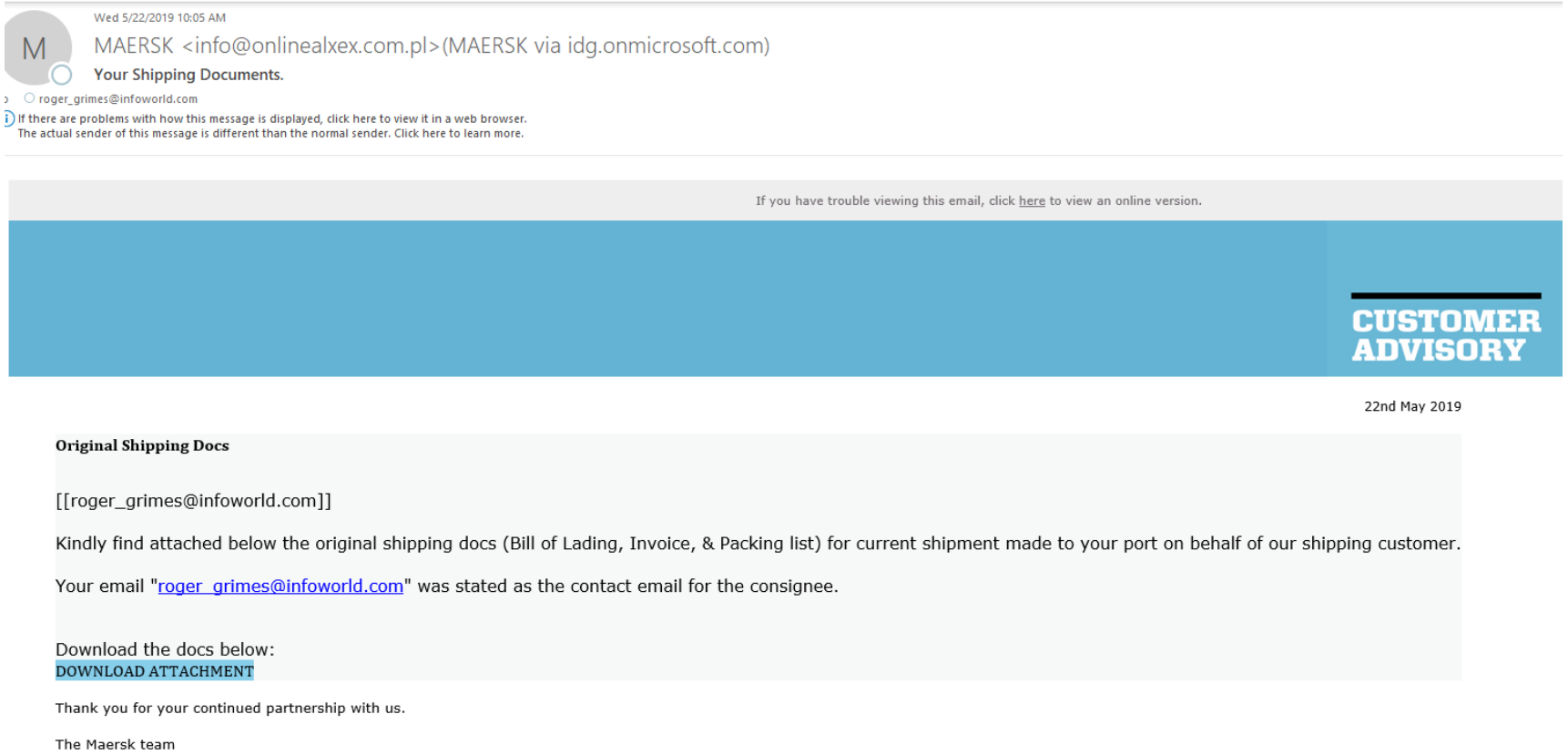
- https://www.ic3.gov/Media/Y2023/PSA230609

Agenda

- Intro to BEC Scams
- Examples of BEC Scams
- Defenses

BEC Scam Examples

Simple and Direct



Wed 5/22/2019 10:05 AM

M

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

Your Shipping Documents.

roger_grimes@infoworld.com

If there are problems with how this message is displayed, click here to view it in a web browser.
The actual sender of this message is different than the normal sender. Click here to learn more.

If you have trouble viewing this email, click here to view an online version.

CUSTOMER ADVISORY

22nd May 2019

Original Shipping Docs

[[roger_grimes@infoworld.com]]

Kindly find attached below the original shipping docs (Bill of Lading, Invoice, & Packing list) for current shipment made to your port on behalf of our shipping customer.

Your email "roger_grimes@infoworld.com" was stated as the contact email for the consignee.

Download the docs below:
DOWNLOAD ATTACHMENT

Thank you for your continued partnership with us.

The Maersk team

BEC Scam Examples

Mortgage Fraud

Money Laundering Email Scam Lands Atlanta Man In Federal Prison

Atlanta man pleaded guilty to money laundering conspiracy for elaborate email spoofing scam aimed at stealing real estate payments.

Marcus K. Garner, Patch Staff

Posted Wed, Jun 2, 2021 at 8:52 am ET | Updated Wed, Jun 2, 2021 at 8:59 am ET

Several days later, on Nov. 1, another homebuyer, this time in Minneapolis, received an email from someone posing as his realtor, providing wiring instructions for a home closing, authorities said. Following the imposter's directions, this victim wired $83,460 to one of King's Atlanta banks, according to prosecutors.

Weeks later, the Delaware law firm received a Nov. 16 email with instructions to wire$68,403 in payoff funds to a mortgage company. That money, instead, went to one of the accounts that King had opened in Atlanta, authorities said. The next day,

https://patch.com/georgia/atlanta/money-laundering-email-scam-lands-atlanta-man-federal-prison

BEC Scam Examples

Posing as Vendor

Feds investigating $1.2 million e-mail fraud scheme that targeted city of Cottage Grove

Scammer allegedly posed as a company contracted for sewer project.

According to five seizure warrant applications signed off on by a federal magistrate judge this month, the fraud involved someone posing as a legitimate company that the city contracted for a sewer project. The fake account convinced the city's accounting specialist to wire money to them and not the real contracted company before the scam was discovered late last year. By the time the fraud was uncovered, the money had been spread to multiple other bank accounts.

https://www.startribune.com/feds-investigating-1-2-million-email-fraud-scheme-that-targeted-city-of-cottage-grove/600199426/

BEC Scam Examples

Compromise Vendor Email and Conduct Scam

PRESS RELEASE

California man who participated in email fraud to steal more than $3 million from boatbuilding companies sentenced to 16 months in prison

According to records filed in the case, including the plea agreement, in October 2018, Redd entered a scheme with a co-conspirator in Pennsylvania and others. The scheme began when a malicious link was sent to an email address of an employee at the engine-building company. The link allowed the conspirators to gain access to the company's email system and review various emails, including those transmitting invoices. The conspirators then posed as a billing executive at the engine manufacturing company and sent the boat-building company instructions to wire the payment funds to a specific bank account. The conspirators had set up a fake company and the account at a Pennsylvania bank specifically to receive these funds. The false emails indicated the engine-building company's usual bank account was undergoing an audit and said that the engine-building company therefore needed to use a different bank than it had previously.

On October 29, 2018, the boat builder paid the invoice for $3,316,730 by wiring the funds as directed by the fraudulent emails. The co-conspirator in Pennsylvania quickly forwarded $3,074,500 to bank accounts controlled by Redd and other co-conspirators. Of the ill-gotten funds, Redd kept $857,350 in accounts he controlled. Investigators were able to seize $420,817 from those accounts.

BEC Scam Examples

Compromise Vendor Email and Conduct Scam

PRESS RELEASE

Previously Extradited Nigerian National Pleads Guilty For His Role In Multimillion-Dollar Business Email Compromise Scheme

Monday, April 8, 2024

For Immediate Release

Court records show that Adeagbo and his co-conspirators obtained information about significant construction projects occurring throughout the United States, including an ongoing multi-million-dollar project at the victim University. To execute the scheme, Adeagbo, Echeazu, and others registered a domain name similar to that of the legitimate construction company in charge of the University's project and created an email address that closely resembled that of an employee of the construction company. Using the fake email address, the fraudsters deceived and directed the University to wire a payment of more than $1.9 million to a bank account controlled by an individual working under the direction of Adeagbo and his co-conspirators. Upon receiving the payment, Adeagbo and his co-conspirators laundered the stolen proceeds through a series of financial transactions designed to conceal the fraud.

BEC Scam Examples

Fake Vendor

More than $100 Million: Google, Facebook Fell for BEC Scam

MON | MAR 25, 2019 | 2:45 PM PDT

A Lithuanian man has this week pleaded guilty to tricking Google and Facebook into transferring over $100 million into a bank account under his control after posing as a company that provided the internet giants with hardware for their data centers.

Fifty-year-old Evaldas Rimasauskas registered and incorporated a company in Latvia with the same name as Quanta Computer, a Taiwan-based electronics manufacturing giant that which been operating since the 1980s.

Knowing that Facebook and Google used Quanta's technology in their data centers, Rimasauskas sent emails to the firms claiming to come from Quanta with forged invoices and fraudulent contracts.

https://www.secureworld.io/industry-news/google-facebook-bec-business-email-compromise

BEC Scam Examples

Fake Vendor

2. Ubiquiti: $46.7m vendor fraud

Ubiquiti is a networking company that lost a staggering $46.7 million due to a BEC scam involving impersonated legitimate vendors.

The incident involved an employee's email impersonation, lax email security, and fraudulent requests from an outside entity targeting the company's finance department to approve money transfers to other overseas accounts held by third parties.

According to Ubiquiti's letter to the SEC that was recently made public, someone at Ubiquiti received phony emails from a bogus Pera and bogus Tom Evans, a lawyer in the London office of Latham & Watkins . The

engineering cyber scam. In its latest SEC filing, the company lays much of the blame on Rohit Chakravarthy, who told the company he would resign as Ubiquiti's chief accounting officer two days before Ubquiti first disclosed the missing money last August. Chakravarthy was promoted into the job only one month before the money went missing, when

https://www.forbes.com/sites/nathanvardi/2016/02/08/how-a-tech-billionaires-company-misplaced-46-7-million-and-didnt-know-it

BEC Scam Examples

Emails From Fake Executive

REUTERS® World Business Markets Sustainability Legal Breakingviews Technology Investigati

World

Scoular hit with $17.2 million fraud: newspaper

By **Reuters**

February 4, 2015 6:02 PM EST · Updated 9 years ago

(Reuters) - Scoular Co, a U.S. grain trading and handling firm, was swindled out of more than $17 million through an international email scheme, a company official confirmed on Wednesday.

The Federal Bureau of Investigation is probing the fraud, which took place in June, a company spokesperson said in a telephone interview.

The Omaha World-Herald newspaper reported the fraud on Wednesday. According to the paper, Scoular sent a total of $17.2 million through three wire transfers in June to a bank in China, acting on emails sent to a Scoular executive.

The emails appeared to be from Scoular Chief Executive Officer Chuck Elsea and the Omaha, Nebraska-based company's auditing firm.

Court documents said the emails were generated by impostors using email addresses set up in Germany, France and Israel and computer servers in Moscow, according to the newspaper.

https://www.reuters.com/article/idUSKBN0L82JV/

BEC Scam Examples

Emails To Executive

Toyota Parts Supplier Loses $37 Million in Email Scam

Posted on September 11, 2019

Toyota Boshoku, a seating and interiors supplier for Toyota cars, has revealed that it was tricked into moving a large amount of money into a bank account controlled by scammers. In a statement published on its global website, Toyota Boshoku Corporation said that its European subsidiary was duped into transferring approximately four billion yen (over US $37 million) out of the business and into a bank account controlled by criminals on 14 August. The company says it became aware of the

https://www.tripwire.com/state-of-security/toyota-parts-supplier-loses-37-million-email-scam

Artificial Intelligence

Overview

- We are already seeing very good AI “deepfakes” used to exploit people
  - “Deepfake” is very realistic, but fake picture, video, or audio recording of a person
- AI used to craft very realistic-looking phishing emails
- AI used to respond to potential victims
- AI used to create “deepfakes” to fool victims
- Create new fake “synthetic” identities

AI-Created Deepfakes Used In Attempt Theft

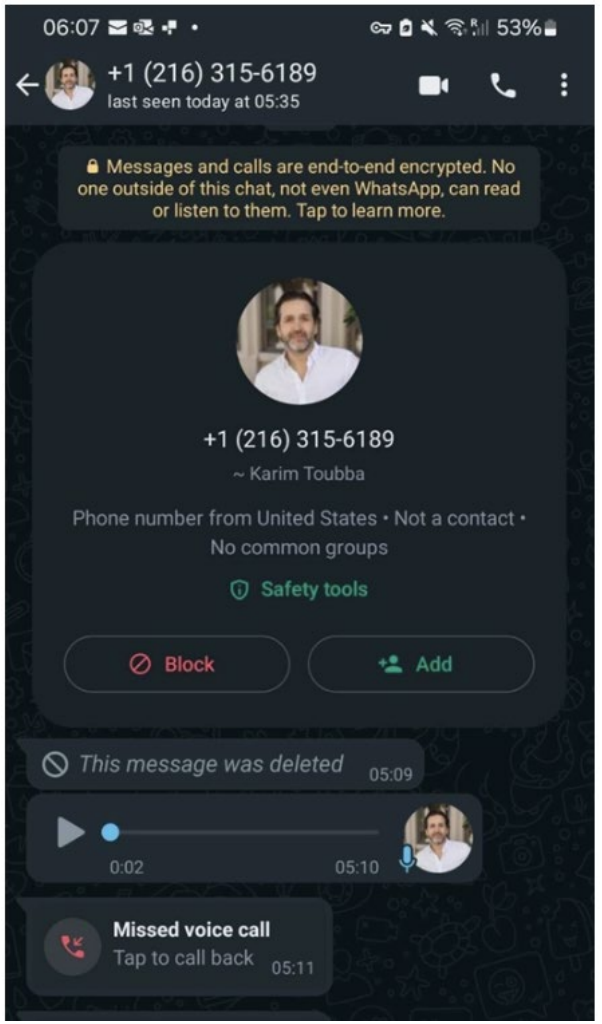
Fake Calls

LASTPASS LABS

Attempted Audio Deepfake Call Targets LastPass Employee

Mike Kosak • April 10, 2024

Mike Kosak, Senior Principal Intelligence Analyst at LastPass, explained in a blog post, "In our case, an employee received a series of calls, texts, and at least one voicemail featuring an audio deepfake from a threat actor impersonating our CEO via WhatsApp.



https://blog.lastpass.com/posts/2024/04/attempted-audio-deepfake-call-targets-lastpass-employee

AI-Created Deepfakes Used In Theft

Fake Calls

FORBES > INNOVATION > CONSUMER TECH

A Voice Deepfake Was Used To Scam A CEO Out Of $243,000

Jesse Damiani Contributor ⓘ

I run the Reality Studies newsletter and Urgent Futures podcast

Follow

Sep 3, 2019, 04:42pm EDT

According to a new report in *The Wall Street Journal*, the CEO of an unnamed UK-based energy firm believed he was on the phone with his boss, the chief executive of firm's the German parent company, when he followed the orders to immediately transfer €220,000 (approx. $243,000) to the bank account of a Hungarian supplier.

In fact, the voice belonged to a fraudster using AI voice technology to spoof the German chief executive. Rüdiger Kirsch of Euler Hermes Group SA, the firm's insurance company, shared the information with WSJ. He explained that the CEO recognized the subtle German accent in his boss's voice—and moreover that it carried the man's "melody."

https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000

AI-Created Deepfakes Used In Theft

Fake Zoom Call

Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’

(CNN) — A finance worker at a multinational firm was tricked into paying out $25 million to fraudsters using deepfake technology to pose as the company’s chief financial officer in a video conference call, according to Hong Kong police.

The elaborate scam saw the worker duped into attending a video call with what he thought were several other members of staff, but all of whom were in fact deepfake recreations, Hong Kong police said at a briefing on Friday.

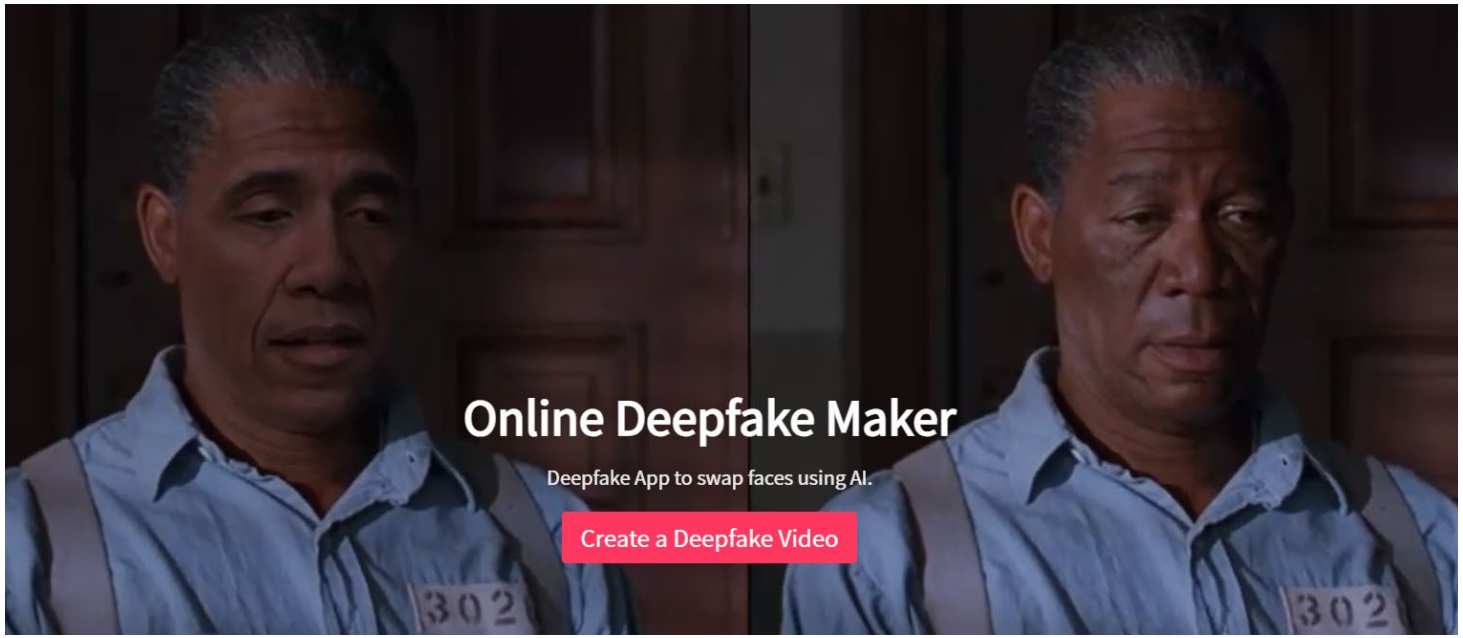
“(In the) multi-person video conference, it turns out that everyone [he saw] was fake,” senior superintendent Baron Chan Shun-ching told the city’s public broadcaster RTHK.

https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html

It’s An Industry Now

Fake Videos

iProov’s research has discovered more than 60 groups dedicated to creating synthetic imagery worldwide, with varying group sizes ranging from 100 to over 100,000 members. One group that focuses on deepfakes boasts a staggering 114,000 members globally. While some groups are interested in technology, others have malicious intent.



https://go.iproov.com/rs/891-TPZ-847/images/iProov%20Threat%20Intelligence_Report.pdf

It’s A Hacker Industry Now

Reused Stolen Biometrics

Step 1:
Steal Biometric Attribute (e.g., face, fingerprint, voice, video, etc.) from victim or video

Step 2:
Create Deepfake

Step 3:
Use Device Emulator to emulate victim’s device (e.g., OS, browser, location, etc.)

Step 4:
Use Virtual Camera
(“camera software” that allows deepfake injection)

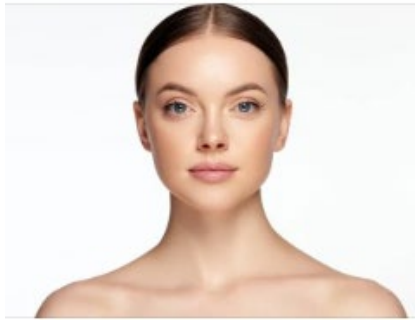
Step 5
Perform Deepfake Attack

It’s Popular Now

Reused Stolen Faces

Hackers and Malware

1. Face swaps are now firmly established as the deepfake of choice among persistent threat actors.
   - We observed an increase in face swap injection attacks of **704%** H2 over H1 2023.

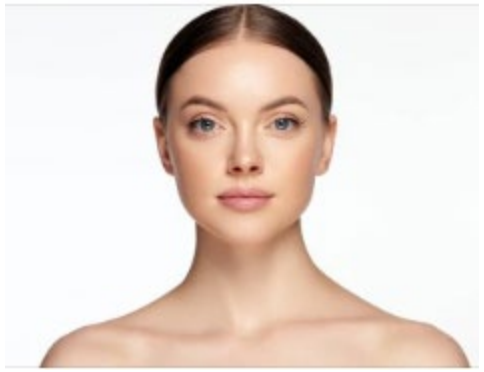


Our analysts continue to track over **110 different face swap tools and repositories.**

https://go.iproov.com/rs/891-TPZ-847/images/iProov%20Threat%20Intelligence_Report.pdf

It’s Automated Now

Reused Stolen Biometrics



Hackers and Malware

Attesting to this, cybersecurity company Group-IB has discovered the first banking trojan that steals people’s faces. Unsuspecting users are tricked into giving up personal IDs and phone numbers and are prompted to perform face scans. These images are then swapped out with AI-generated deepfakes that can easily bypass security checkpoints

The method — developed by a Chinese-based hacking family — is believed to have been used in Vietnam earlier this month, when attackers lured a victim into a malicious app, tricked them into face scanning, then withdrew the equivalent of $40,000 from their bank account.

https://www.linkedin.com/pulse/game-changer-biometric-stealing-malware-roger-grimes-ikaze

Conclusion

Reused Stolen Biometrics

Manual remote identity verification has been proven ineffective. With the emergence of advanced technologies such as generative AI and face swaps, identity fraud has become a significant concern for organizations.

STAMFORD, Conn., February 1, 2024

Gartner Predicts 30% of Enterprises Will Consider Identity Verification and Authentication Solutions Unreliable in Isolation Due to AI-Generated Deepfakes by 2026

https://www.gartner.com/en/newsroom/press-releases/2024-02-01-gartner-predicts-30-percent-of-enterprises-will-consider-identity-verification-and-authentication-solutions-unreliable-in-isolation-due-to-deepfakes-by-2026

Agenda

- Intro to BEC Scams
- Examples of BEC Scams
- Defenses

Best Defenses

Defenses – The Hartford

https://sba.thehartford.com/business-management/email-compromise

- **Implement ETF Policies That Defeat BEC Scams**
- All unexpected requests must be confirmed using an alternative, trusted, method
- Never use phone numbers or email addresses in or from originating email

Best Defenses

Defenses – The Hartford

https://sba.thehartford.com/business-management/email-compromise

- Look for “red flags”

- **Look-alike or different reply-to addresses.** Scammers might send an email from an address that looks very similar to your company’s email, such as ceo@c0mpany.com instead of ceo@company.com. Or, they can make the from-address look exactly like your company’s, but the reply-to address is the scammer’s email account.
- **Short messages that create a sense of urgency.** A low- or mid-level employee might want to quickly and unquestioningly respond to urgent requests from an executive. But make sure everyone knows it’s okay to ask questions when there’s a request for money or personal information.
- **A need for secrecy.** The scammers could also use a false pretense to keep recipients from asking others for advice. For example, the scammer might ask your assistant to buy 15 gift cards and not tell anyone because they’re going to be surprise thank you gifts for the team.
- **Unusual timing.** The attack could start during off-hours or a holiday, which plays into the idea that it’s an urgent request and could keep the recipient from verifying details with others.
- **Requests for changing account information.** A change in the payment instructions, direct deposit forms or other account information could be legitimate, but it’s also a red flag. Try to verify the request by phone using a number that’s not listed in the email.

Best Defenses

Defenses – The Hartford

https://sba.thehartford.com/business-management/email-compromise

- **Have a security awareness training program**
- **Educate yourself and others on what to look out for**
- **Always confirm where email came from (especially the sender's domain)**

- **How to Spot Rogue URLs**
  - https://blog.knowbe4.com/top-12-most-common-rogue-url-tricks
  - https://info.knowbe4.com/rogue-urls

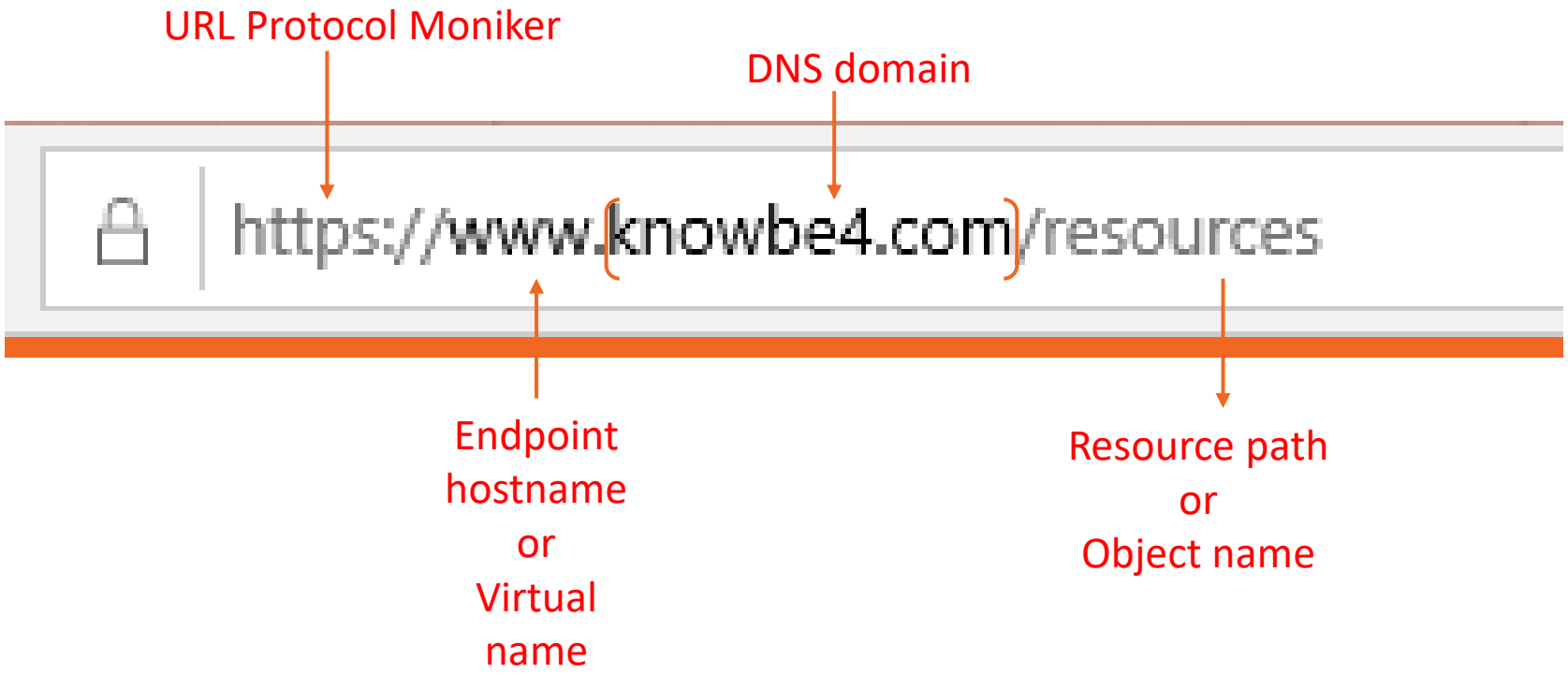
Understanding URLs

So, you think you understand everything about URL links?

Let’s see…

Understanding URLs

Basics



Understanding URLs

URL Protocol Monikers

- http://
- https://
- ftp://
- data://
- file://
- mailto://
- telnet://
- uri://
- ssh://
- tel://
- javacript://
- tn3270://
- custom://
  - whatever you want to make

Understanding URLs

Basics

DNS hostname

- Starts after double forward slashes
- Ends before first period

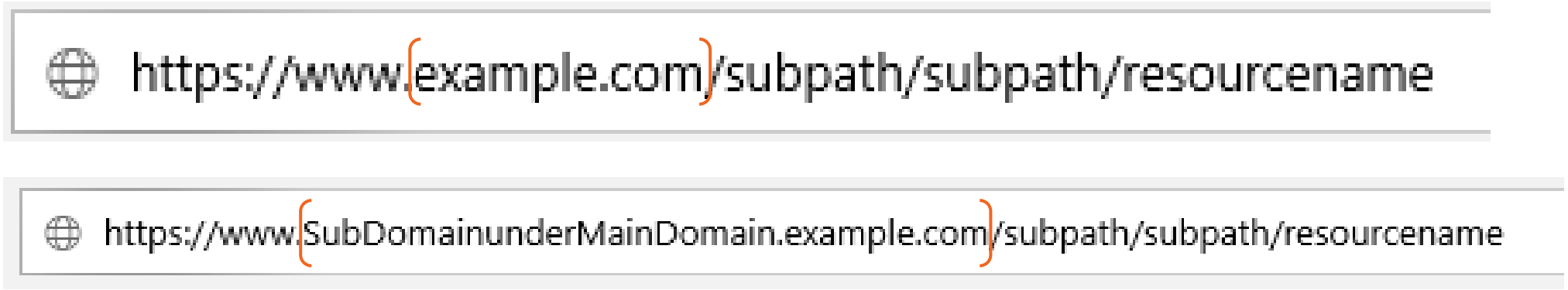
- Can be “real” hostname or virtual
- May not be present in URL
  - If missing, default hostname will be tried

Understanding URLs

Basics

DNS domain name

- Starts after first period after hostname
- Ends at before first single slash



Understanding URLs

Basics

DNS Top-Level Domain (TLD) name

- Starts forward from last period before first slash
- Ends before first slash

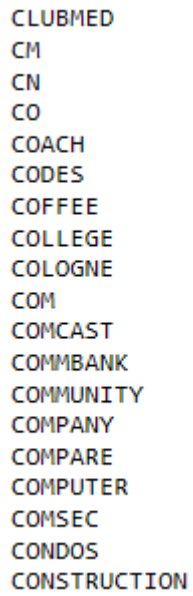
- There are thousands of TLD domain names
- Ex: com, org, pub, gov, mil, biz, etc.

Understanding URLs

Basics

DNS Top-Level Domain (TLD) name

- Most are 2-4 characters, but there are all sorts of lengths today
- Two-digit country code (e.g. au, ch, ru, etc.)
- Not all apps support all TLDs
- Some TLDs more risky than others
- TLD names are controlled by IANA
  - http://data.iana.org/TLD/tlds-alpha-by-domain.txt



Understanding URLs

Basics

Resource path name

- Starts after first single slash
- Ends at last slash

Understanding URLs

Basics

Resource name

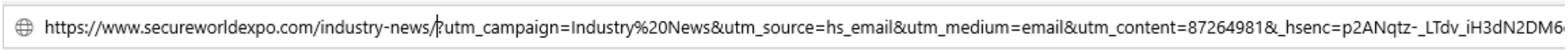
- Starts after last slash
- Refers to file name of object being called
  - File, graphic, web page, etc.
  - Optional, and may or may not include extension
  - Default doc (index.htm[l]) will be tried if missing

Understanding URLs

Basics

- Anything after the first **?** is a **variable** being passed back to the host to be evaluated
- Often used to track users

Everything after ? is a variable

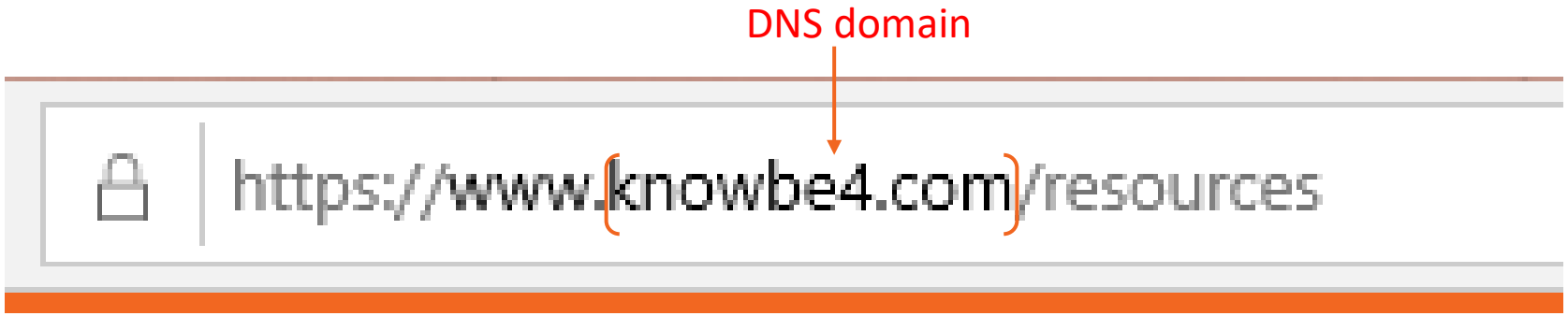


multiple variables separated by &

Understanding URLs

Basics

- Most important URL analysis skill you can know or teach is how to figure out what the true DNS domain is



Understanding URLs

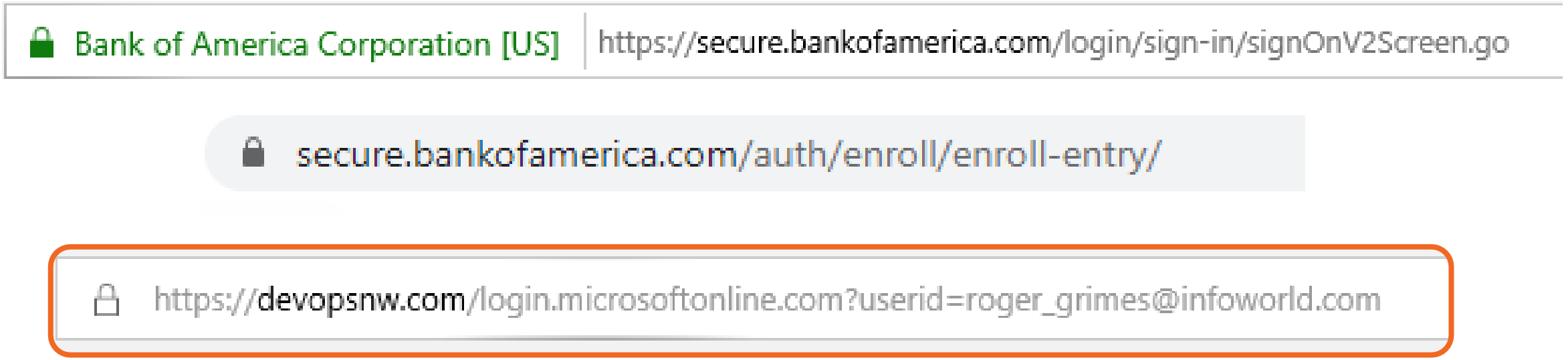
Basics

- Most important URL analysis skill you can know or teach is there is big difference between:

Understanding URLs

Basics

- Some browsers will **highlight** the real DNS hostname and domain to help with review



Common URL Phishing Tricks

Spotting Rogue URLs – Look-Alike Domains

original*	knowbe4.com
insertion	knowsbe4.com
hyphenation	know-be4.com
transposition	konwbe4.com
insertion	knownbe4.com
transposition	knoweb4.com
replacement	knowber.com
repetition	knowbee4.com
replacement	knowb34.com
insertion	knowebe4.com
insertion	knowbne4.com
transposition	knowb4e.com

insertion	knkowbe4.com
insertion	knbowbe4.com
insertion	kbnowbe4.com
bitsquatting	onowbe4.com
omission	nowbe4.com
replacement	mnowbe4.com
omission	kowbe4.com
omission	knwbe4.com
replacement	knpwbe4.com
replacement	knowne4.com
replacement	knowhe4.com
omission	knowe4.com

replacement	knowbw4.com
bitsquatting	knowbu4.com
replacement	knowbs4.com
replacement	knowbr4.com
vowel-swap	knowbo4.com
insertion	knowbe44.com
bitsquatting	knowbd4.com
repetition	knowbbe4.com
replacement	knoqbe4.com
omission	knobe4.com
replacement	knoabe4.com
bitsquatting	knkwbe4.com
vowel-swap	knewbe4.com

From our **Domain Doppelganger** tool https://www.knowbe4.com/domain-doppelganger

Common URL Phishing Tricks

Spotting Rogue URLs – Look-Alike Domains

Subdomain tricks

domain
is
paypal.com.bank
Not
paypal.com

Common URL Phishing Tricks

Spotting Rogue URLs – Bait & Switch Domains

Subdomain tricks

domain
is
microsoft.co.login-update-dec20.info
not
microsoft.co
or
Microsoft.com

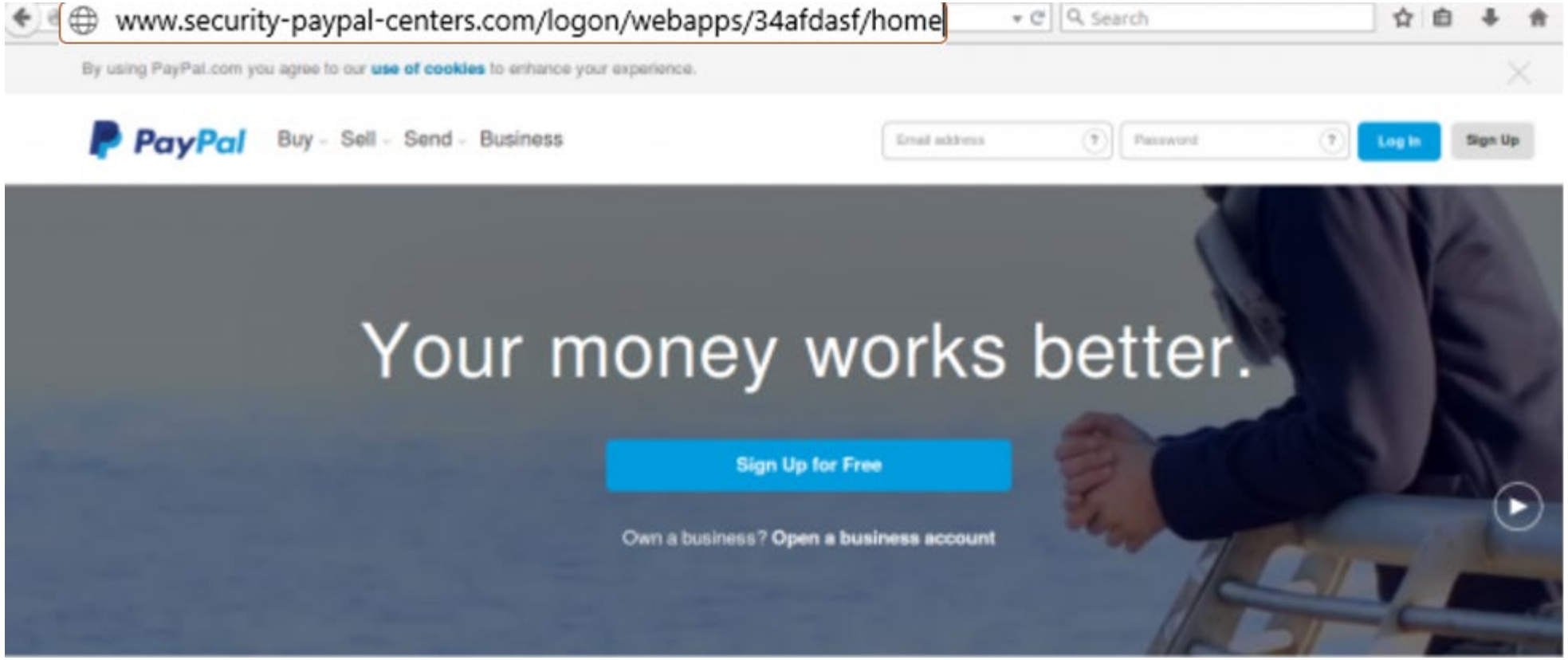
Common URL Phishing Tricks

Spotting Rogue URLs – Look-Alike Domains

parent domain is **doc.com**

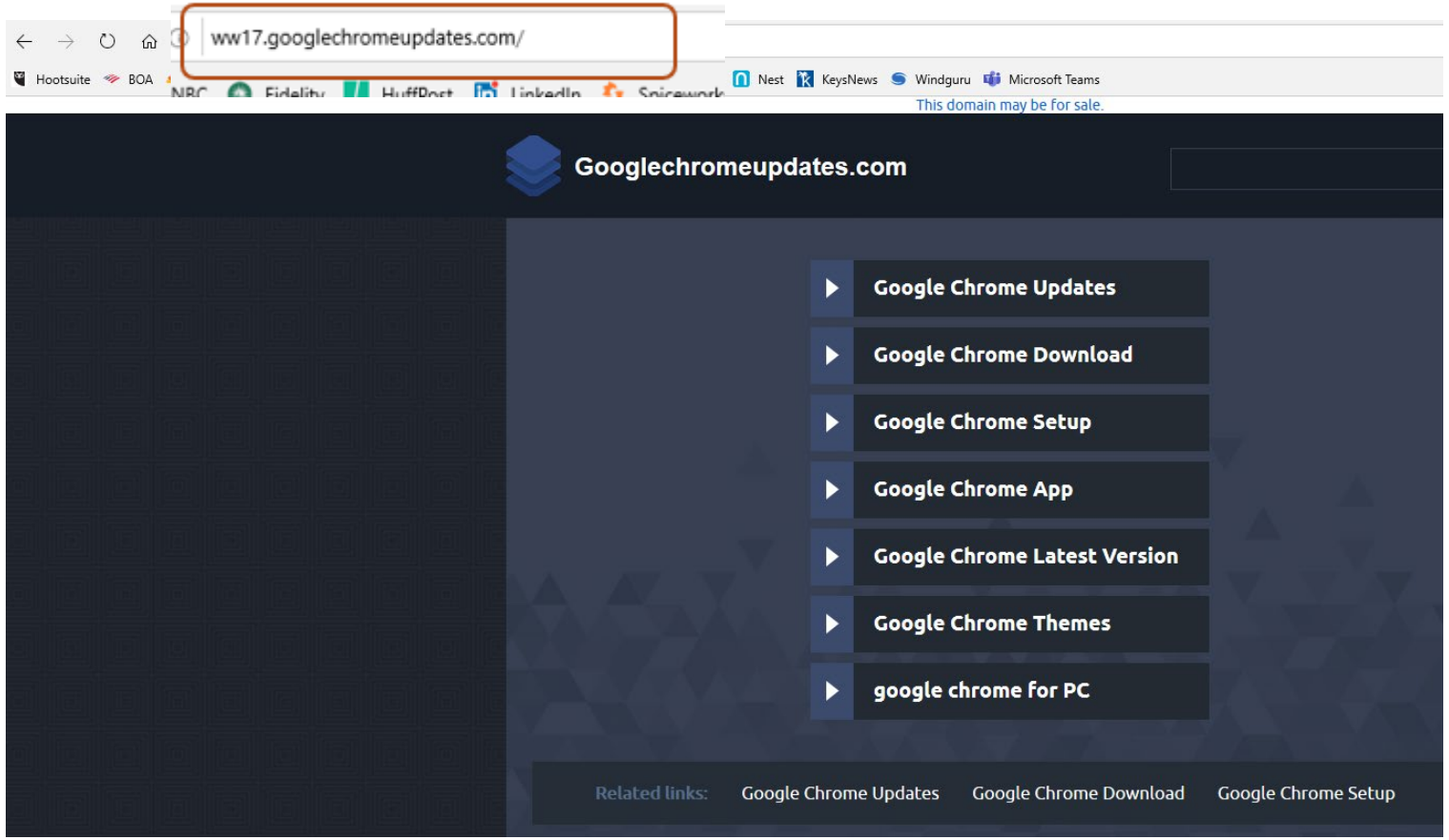
Common URL Phishing Tricks

Spotting Rogue URLs – Look-Alike Domains



Common URL Phishing Tricks

Spotting Rogue URLs – Look-Alike Domains

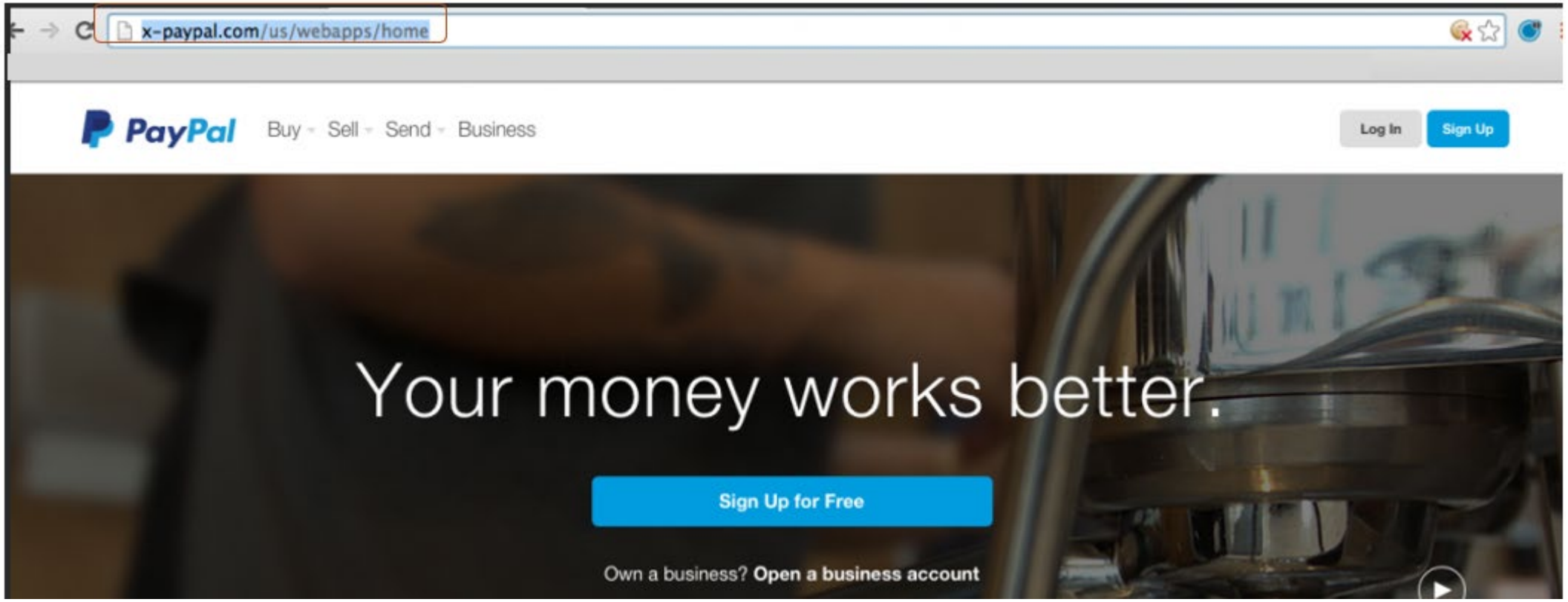


googlechromeupdates.com is not owned by Google

Common URL Phishing Tricks

Spotting Rogue URLs – Look-Alike Domains

x-paypal.com is not **paypal.com**



Common URL Phishing Tricks

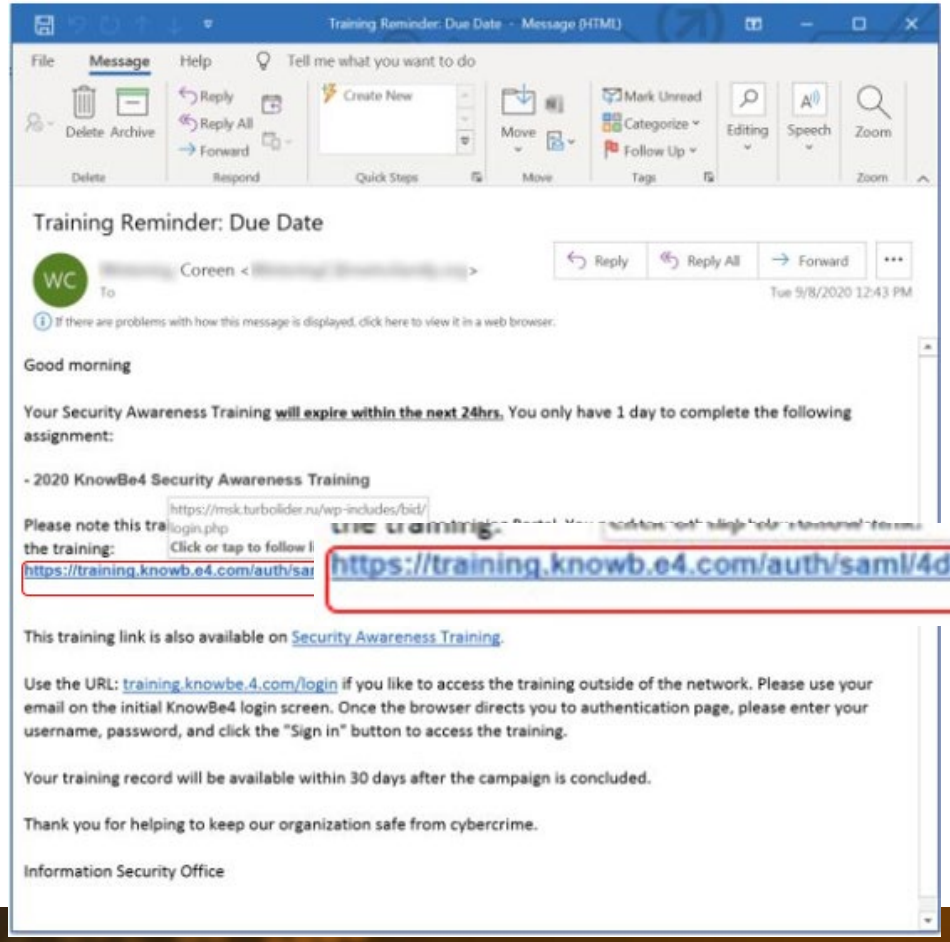
Spotting Rogue URLs – Look-Alike Domains

Please! This is a public plea as we need HELP: Footage has been uploaded of the suspect that ran over one of my relatives yesterday at one of our local gas stations in which the suspect is seen getting into an argument with a group of people inside before attempting to run them over after they are seen exiting the store. My cousin was at the wrong place at the wrong time and was killed on the spot as the suspect is seen ramming his truck into the group. The person is seen fleeing in an unmarked licensed plate vehicle, a reward of $35,000 has been set to identify this person. If you recognize this person please contact your local authorities asap! Video 1:31 minutes - https://cnnnewsalert133.wixsite.com/alert/?aa19

wixsite.com
is not
cnn.com

Common URL Phishing Tricks

Spotting Rogue URLs – Look-Alike Domains



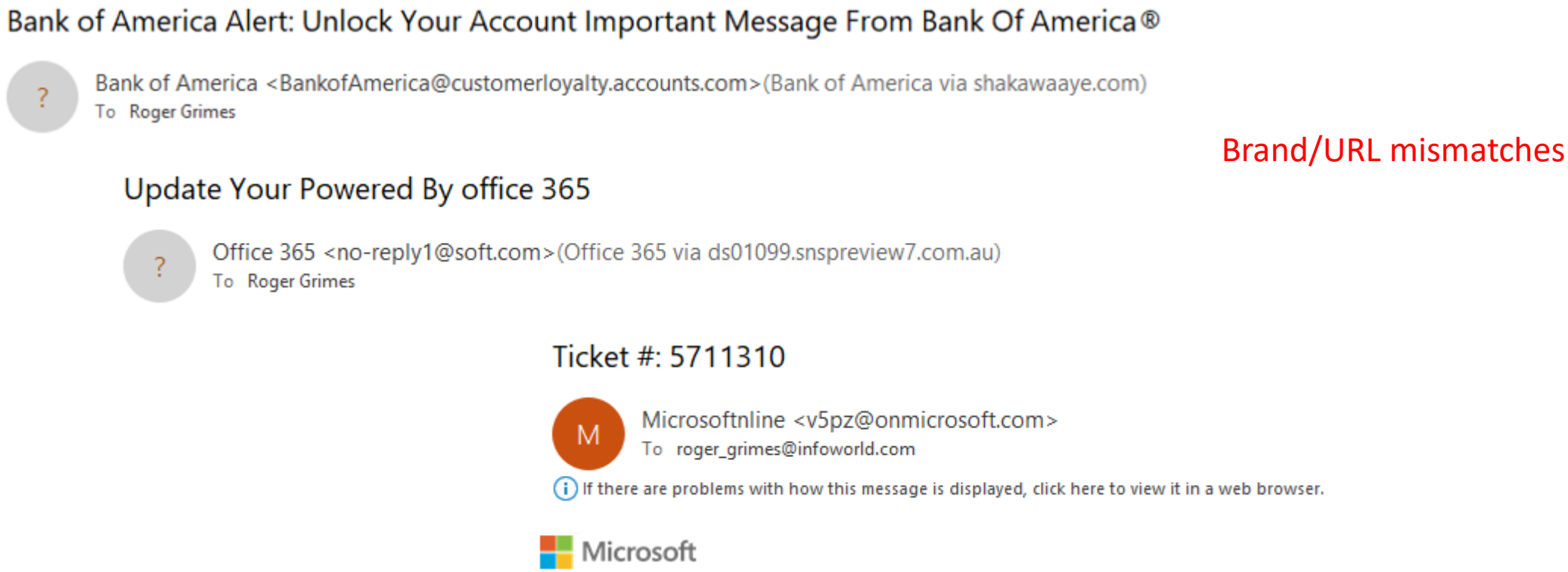
parent domain
is
e4.com
not
knowbe4.com

Common URL Phishing Tricks

Spotting Rogue URLs – Look-Alike Domains

Common URL Phishing Tricks

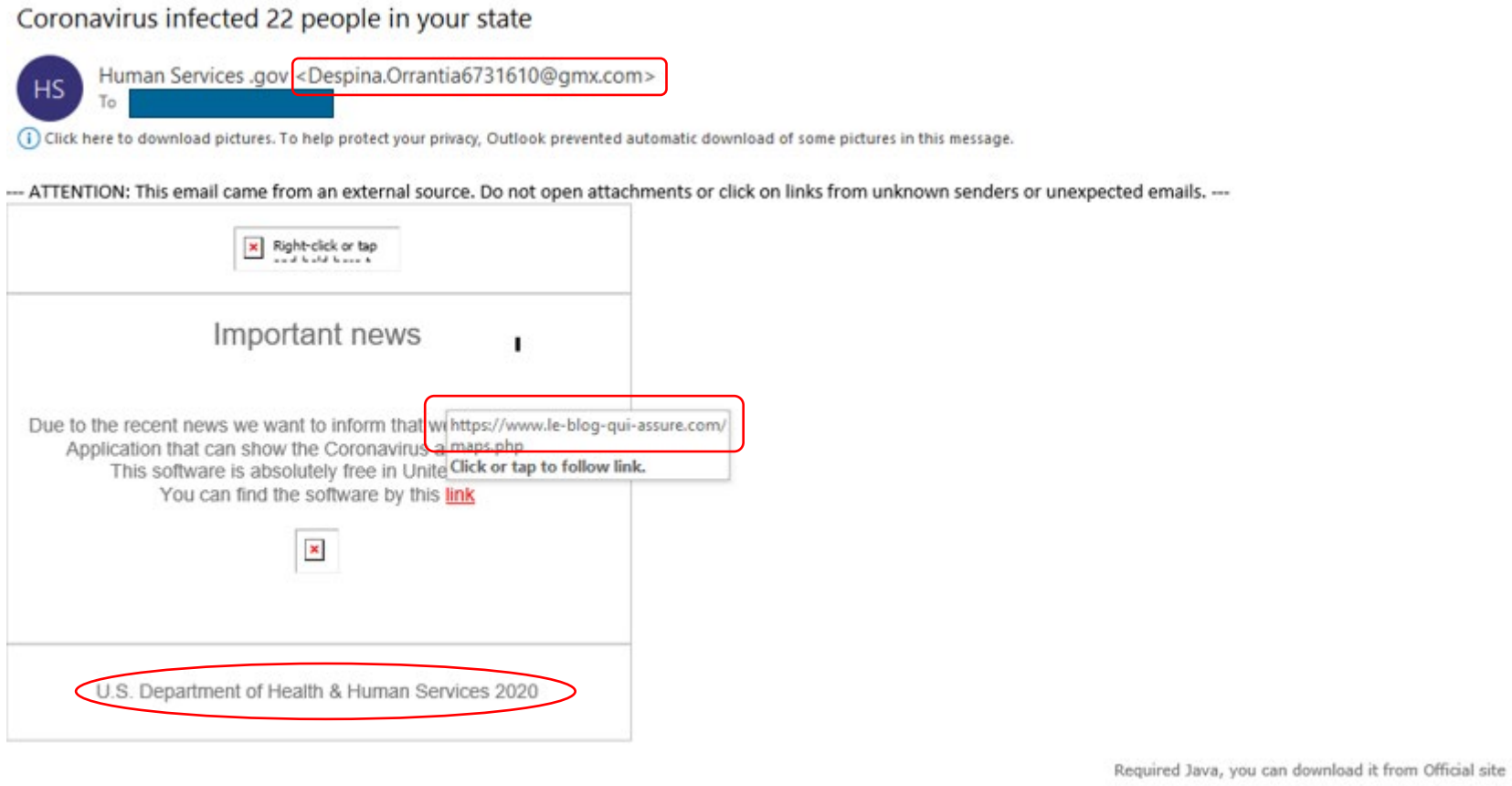
Spotting Disconnected Email Addresses



Brand/URL mismatches

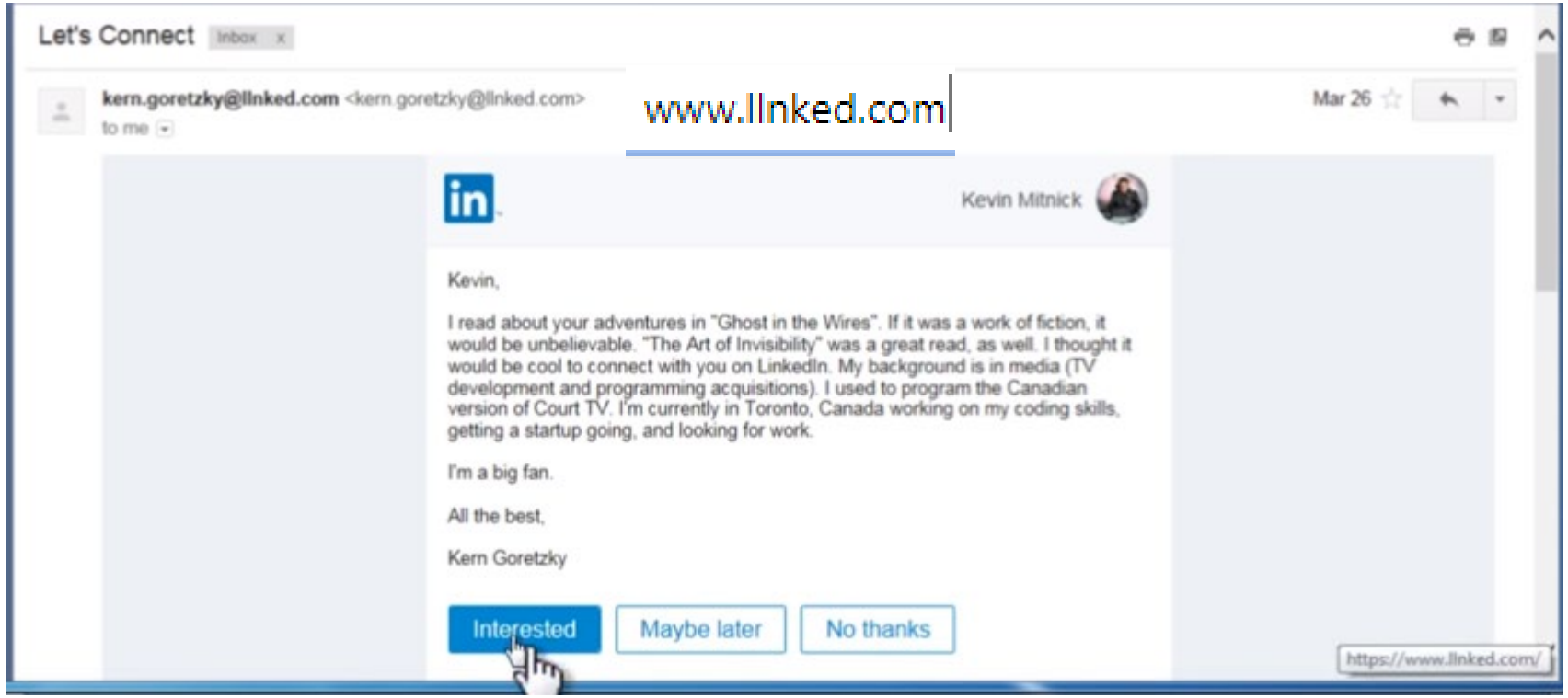
Common URL Phishing Tricks

Spotting Rogue URLs – Domain Mismatches



Common URL Phishing Tricks

Spotting Rogue URLs – Slightly misspelled



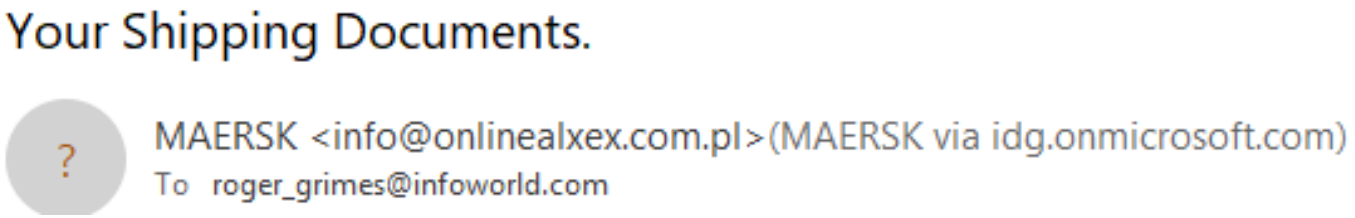
Common URL Phishing Tricks

Strange Origination Domain

Be wary of any large company not using their own domain name

Examples

- Hotmail.com
- Gmail.com
- Onmicrosoftonline.com



Best Defenses

Defenses – The Hartford

https://sba.thehartford.com/business-management/email-compromise

- **Use Multifactor Authentication (MFA)**
- **Use PHISHING-RESISTANT MFA, whenever possible!**

Articles

- **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

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

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

Best Defenses

Defenses – The Hartford

https://sba.thehartford.com/business-management/email-compromise

- **Implement DMARC, SPF, and DKIM**

- **Understanding DMARC**
  - https://info.knowbe4.com/dmarc-spf-dkim-webinar (1-hour free webinar)
  - https://www.linkedin.com/pulse/understanding-dmarc-better-roger-grimes/ (article)

DMARC, DKIM, SPF

Global Phishing Protection Standards

- **Sender Policy Framework (SPF)**
- **Domain Keys Identified Mail (DKIM)**
- **Domain-based Message Authentication, Reporting and Conformance (DMARC)**
- Helps prevents sender email domain spoofing
- Senders: Helps protect YOUR domain against spoofing by others!
- Receivers: Verifies whether or not an email that claims to be from a particuar domain is really from that domain
- Typically happens on email servers and agents, user is unaware it's happening

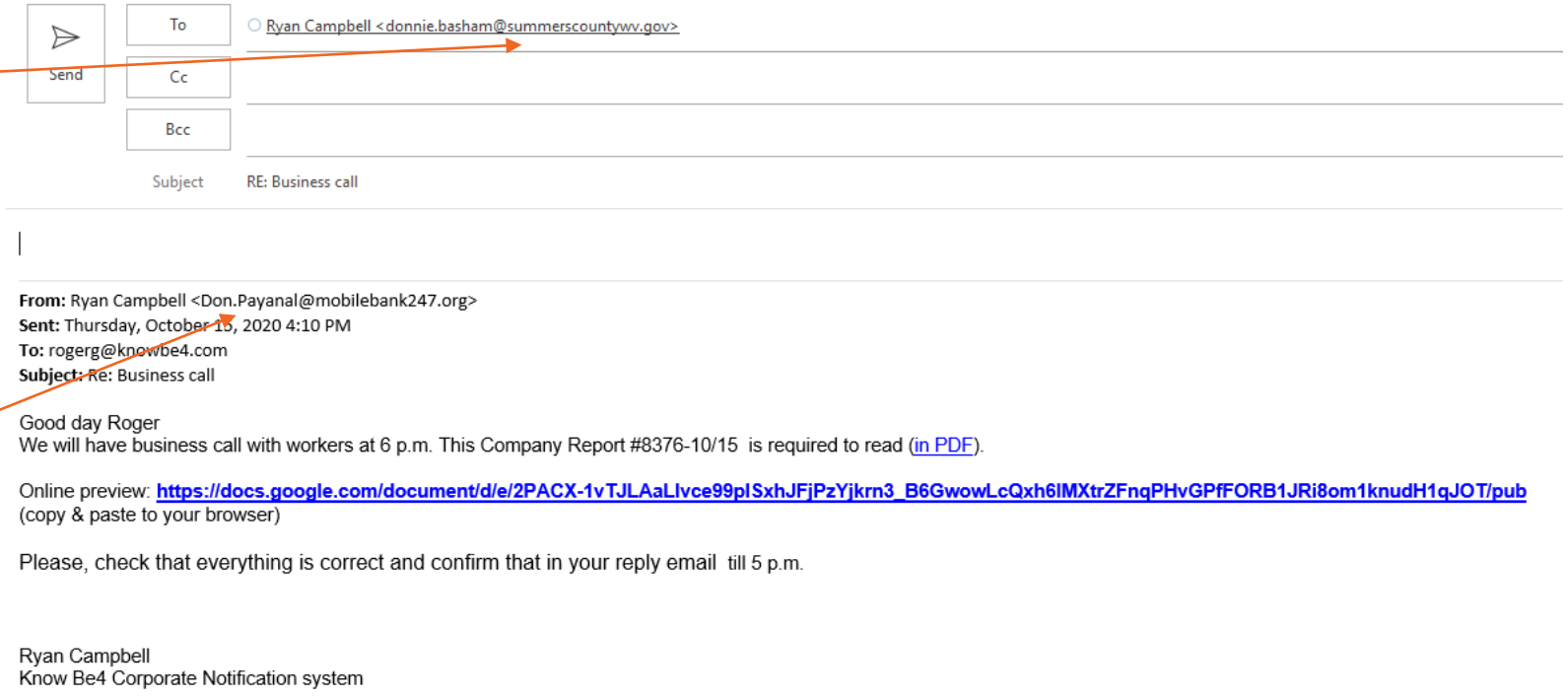
SPF & DKIM

Global Email Authentication Standards

- **Sender Policy Framework (SPF)**
  - Verifies the 5321 **MAIL FROM/RECPT To** domain name address

5321.MAIL FROM domain

not 5322.DISPLAY FROM domain



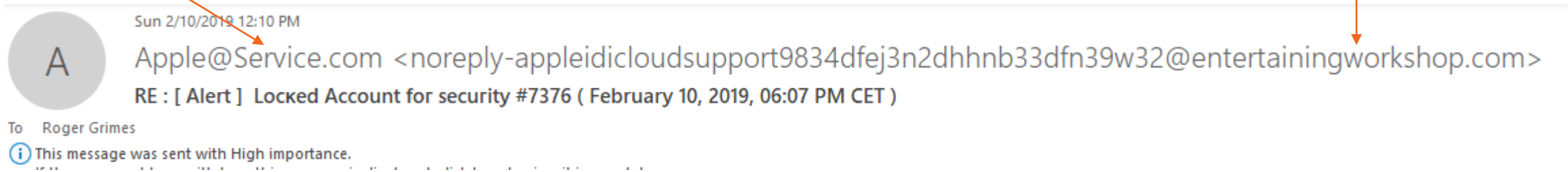
SPF & DKIM

Global Email Authentication Standards

- **Sender Policy Framework (SPF)**
  - Verifies the 5321 **MAIL FROM/RECPT To** domain name address
    - This is the “real” return email address that <u>you see just opening an email</u>

“Friendly From Name”
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 add a digital signature to every outgoing email that links the email to its sending Internet domain
    - DKIM signatures typically cover most of the email message to verify message hasn't been adulterated between sending and receiving

```
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=iVrm4GcK3W8w6dNUvDCTJY22HJmChvuZ7JCebDsftOg=;
        b=CVIqiyEdtNmyvl8PAbimb87xBL15wQPS2k89oEg14uz4LugQLf3U/Vw7GpRLciiRO+
         dCpszAlw0WNWBGcRmJKM/dzLwTR6wTth/vwkXpcf8tT2/K9c1Le649YRnwtdnwmNwpxu
         PEqzATj0uj6hiEUmy4UL1/e6tP58Gb5UMCKpsXdV1+J3Qu3Jech7k5250LQRLqsVetAE
         G7fCQ6GFpaAApnRXa2BTOk7gHPB4Ak8BYy7iNT2ckuPi7ETuCaA4bqplKpm5LlpsTKUW
         x/gAsB94w5fv5Q+UTZhiz3LTEz1YMh5UEi8Ix+O2mUMTBXgINpmxV9MqdF0AhVyC1uef
         NTHw==
```

DMARC

DMARC Status

```
Authentication-Results: spf=pass (sender IP is 65.39.215.30)
 smtp.mailfrom=mx.sailthru.com; dkim=pass (signature was verified)
 header.d=vox.com;dmarc=pass action=none header.from=vox.com;compauth=pass
 reason=100
```

- **Pass**
  - Passes DMARC and/or SPF, and/or DKIM, no failures
- **Fail**
  - Fails DMARC alignment, and/or SPF, and/or DKIM, maybe no policies defined

```
header.d=amazonses.com;dmarc=fail action=none
```

- **None**
  - No policies defined

```
Authentication-Results: spf=none (sender IP is 207.134.53.58)
 smtp.mailfrom=inreachitsolutions.com; banneretcs.com; dkim=none
(message not
 signed) header.d=none;banneretcs.com; dmarc=none action=none
 header.from=inreachitsolutions.com;
Received-SPF: None (protection.outlook.com: inreachitsolutions.com does
not
```

Best Defenses

Real Estate Scam Defenses

- Education for all involved
- Don’t put full wire transfer information on any email correspondence or documentation
- Require people to call known good phone number to get full wiring instructions on day of transfer

Best Defenses

Incident Response – The Hartford

https://sba.thehartford.com/business-management/email-compromise

If you are the victim of a BEC scam:

- Immediately contact your financial institution to see if it can reverse the transfers or payments
- If needed, work with your IT team to make sure your devices and accounts
- Notify your insurance provider as soon as possible
- Report the incident to the FBI's Internet Crime Complaint Center.
  https://www.ic3.gov/Home/BEC

Platform for Awareness Training and Testing

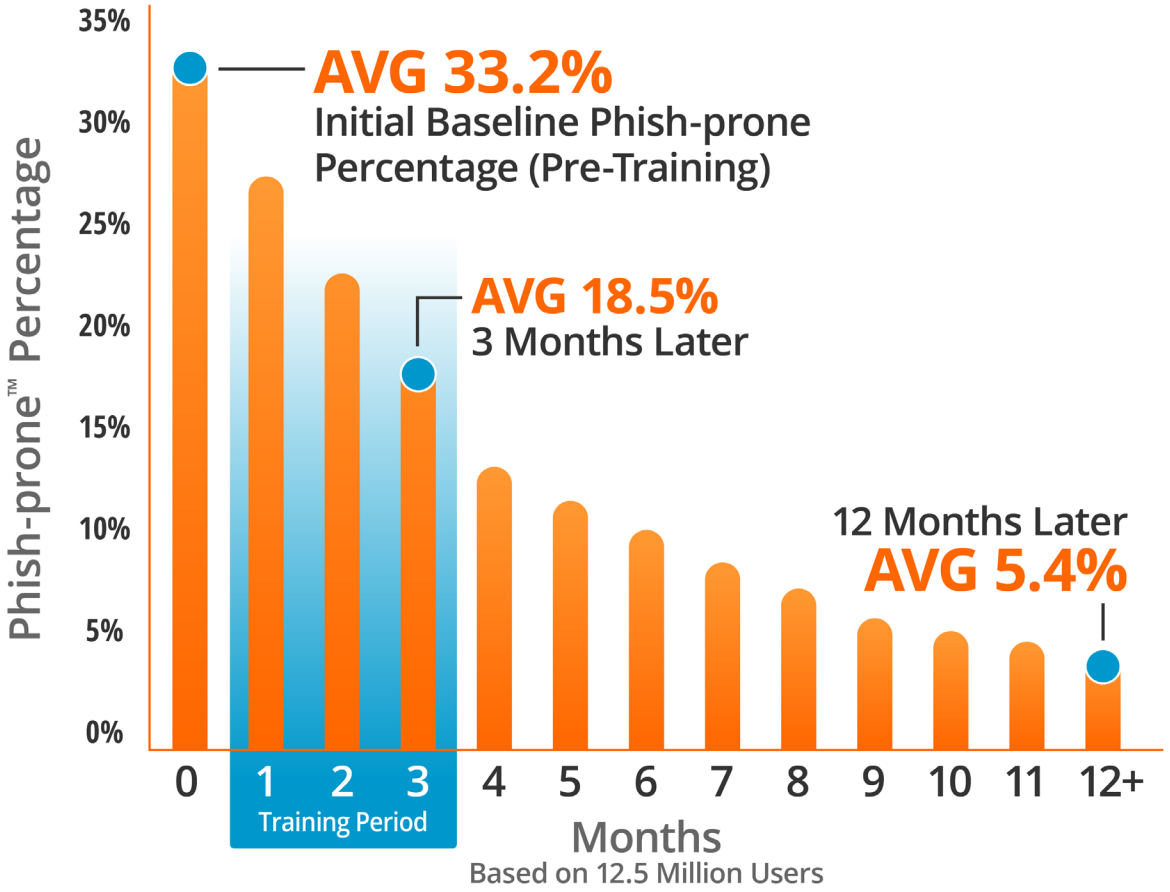
1. Train Your Users
2. Phish Your Users
3. See the Results

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

82% Average Improvement

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



Source: 2023 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.

Reduce The Risk to Social Engineering & Phishing

The Hartford partnership with KnowBe4 earns you exclusive discounts* on the only platform truly dedicated to improving organizational security culture and reducing human risk

With KnowBe4 you can:

- Send fully automated simulated phishing attacks
- Train your users with access to the world's largest library
- AI-driven phishing and training recommendations
- Use assessments to gauge proficiency of your users in security knowledge and security culture attitudes
- Easy user management using Active Directory or SCIM integration

Get a personalized demo: https://www.knowbe4.com/hartford-offer

* 25% discount on KnowBe4 Security Awareness Training platform and 20% discount on PhishER, SecurityCoach and Compliance Plus
*Terms and conditions apply

Questions?

Roger A. Grimes– Data-Driven Defense Evangelist, KnowBe4
e: rogerg@knowbe4.com
LinkedIn: https://www.linkedin.com/in/rogeragrimes/
Mastodon: https://infosec.exchange/@rogeragrimes
Twitter: @RogerAGrimes

Disclaimer

The information provided in these materials is intended to be general and advisory in nature. It shall not be considered legal advice. The Hartford does not warrant that the implementation of any view or recommendation contained herein will: (i) result in the elimination of any unsafe conditions at your business locations or with respect to your business operations; or (ii) be an appropriate legal or business practice. The Hartford assumes no responsibility for the control or correction of hazards or legal compliance with respect to your business practices, and the views and recommendations contained herein shall not constitute our undertaking, on your behalf or for the benefit of others, to determine or warrant that your business premises, locations or operations are safe or healthful, or are in compliance with any law, rule or regulation. Readers seeking to resolve specific safety, legal or business issues or concerns related to the information provided in these materials should consult their safety consultant, attorney or business advisors. All information and representations contained herein are as of June 2024.

The Hartford Financial Services Group, Inc., (NYSE: HIG) operates through its subsidiaries, including the underwriting company Hartford Fire insurance Company, under the brand name, The Hartford®, and is headquartered in Hartford, CT. For additional details, please read The Hartford's legal notice at www.thehartford.com