KnowBe4
Human error. Conquered.

Spotting and Defending Against BEC Tax Scams

James McQuiggan
Security Awareness Advocate,
KnowBe4, Inc.

Erich Kron
Security Awareness Advocate,
KnowBe4, Inc.

Housekeeping

- If you are having audio or video issues, refreshing your browser usually will fix any problems
- Chrome is the best browser to use if possible
- This presentation is being recorded and will be available on-demand after the broadcast
- The slides and all mentioned resources are available for download in the resources box in your webinar console
- There is a team behind the scenes ready to answer your questions, and we will get to some if there is time at the end, so please send questions in the Q&A box in your webinar console

Erich Kron

Security Awareness Advocate

About Erich Kron

- CISSP, CISSP-ISSAP, MCITP, ITIL v3, etc…
- Former Security Manager for the US Army 2nd Regional Cyber Center – Western Hemisphere
- Former Director of Member Relations and Services for (ISC)^2
- A veteran of IT and Security since the mid 1990's in manufacturing, healthcare and DoD environments

CISSP® Certified Information Systems Security Professional

CISSP® Certified Information Systems Security Professional

ISSAP® Architecture

Microsoft® CERTIFIED IT Professional

KnowBe4
Human error. Conquered.

James R. McQuiggan, CISSP

Security Awareness Advocate

KnowBe4
Human error. Conquered.

About James

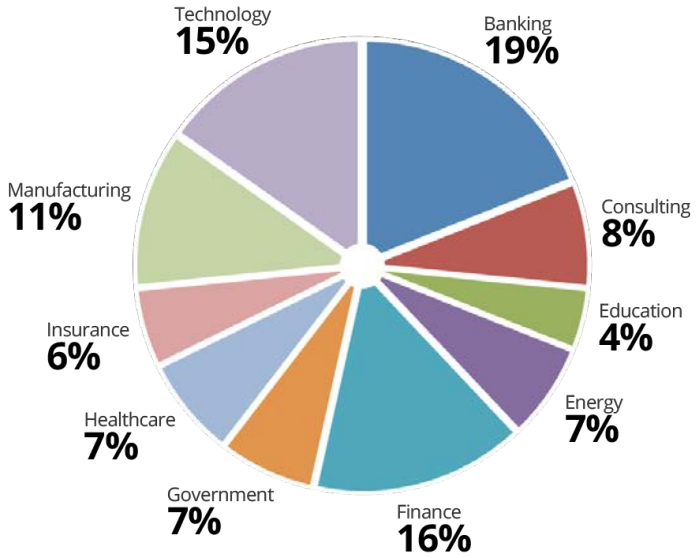
- Security Awareness, Siemens Energy
- Product Security Officer, Siemens Gamesa
- Adjunct Professor, Valencia College
- (ISC)^2 Central Florida Chapter President
- Board of Trustees, Center for Cyber Safety & Education
- Leadership Board, InfoSec World Conference & Expo

CISSP® Certified Information Systems Security Professional

CENTER FOR CYBER SAFETY AND EDUCATION™

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



Agenda

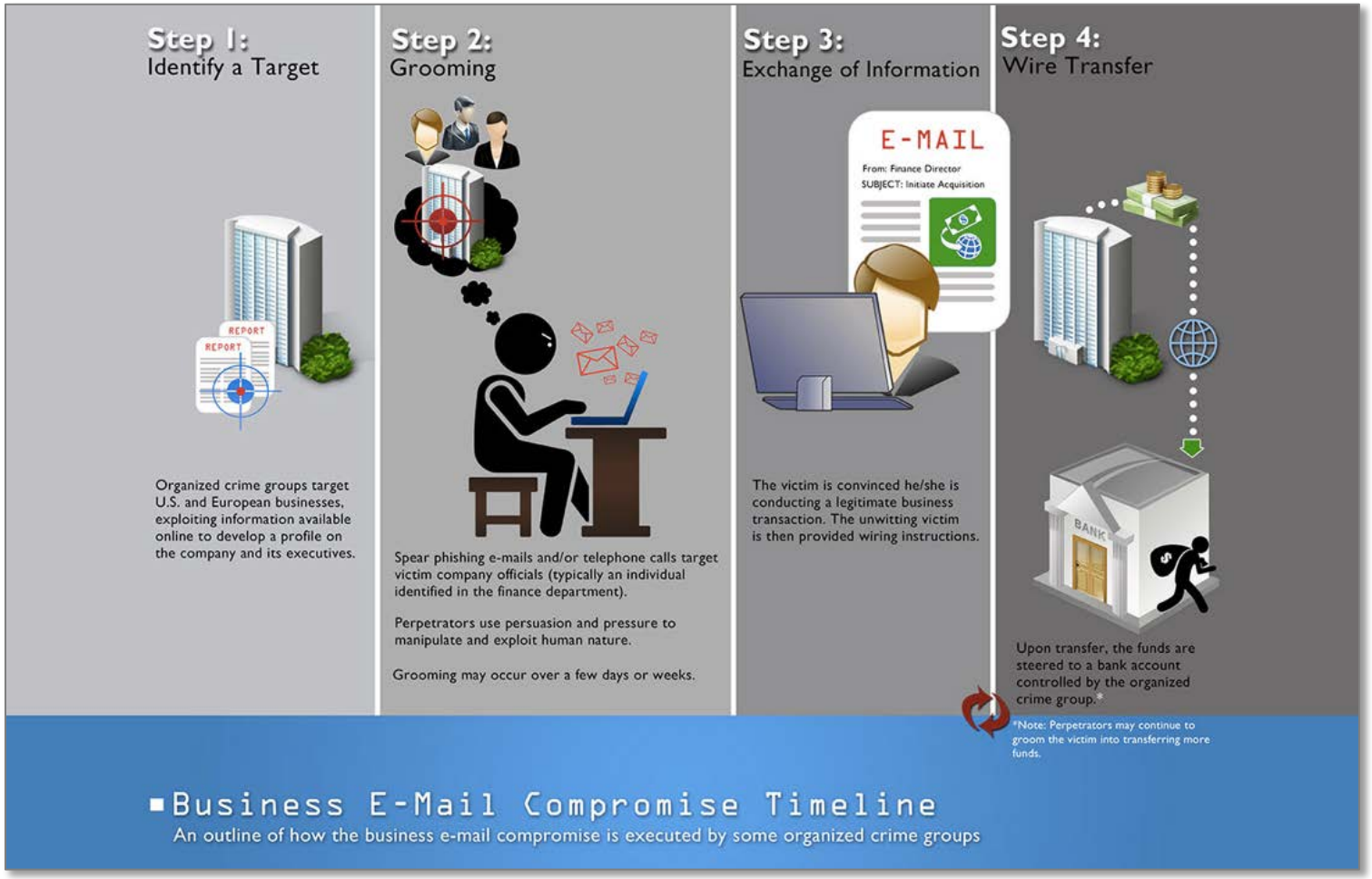
- What is BEC?
- Tax themed attack types
- Common targets within your organization
- Defending against the attacks

Agenda

- What is BEC?
- Tax themed attack types
- Common targets within your organization
- Defending against the attacks

Business Email Compromise

At its heart, BEC relies on the oldest trick in the con artist's handbook: deception. But the level of sophistication in this multifaceted global fraud is unprecedented, according to law enforcement officials, and professional businesspeople continue to fall victim to the scheme. - fbi.gov



Business Email Compromise (BEC)

BEC scams usually target money or information by using the authority of an executive to get people to take an action.

Wire Transfer Fraud

W2 Fraud

Gift card Fraud

Attackers may start the attacks from within the executive's real email account, they may spoof the reply address, or they might even just use a generic address.

CEO Fraud and BEC Causes $26 Billion in Damages

There are various versions of the scams. Victims range from large corporations to tech companies to small businesses to non-profit organizations. Many times, the fraud targets businesses that work with foreign suppliers or regularly perform wire transfer payments.

- Law enforcement globally has received complaints from victims in every U.S. state and in at least 177 countries.
- FBI Alert Number I-091019-PSA puts the losses at over $26 billion between October 2013 and July 2019.
- Between May 2018 and July 2019, there was a 100% increase in identified losses.

Why are you being manipulated?

-- understand the lures --

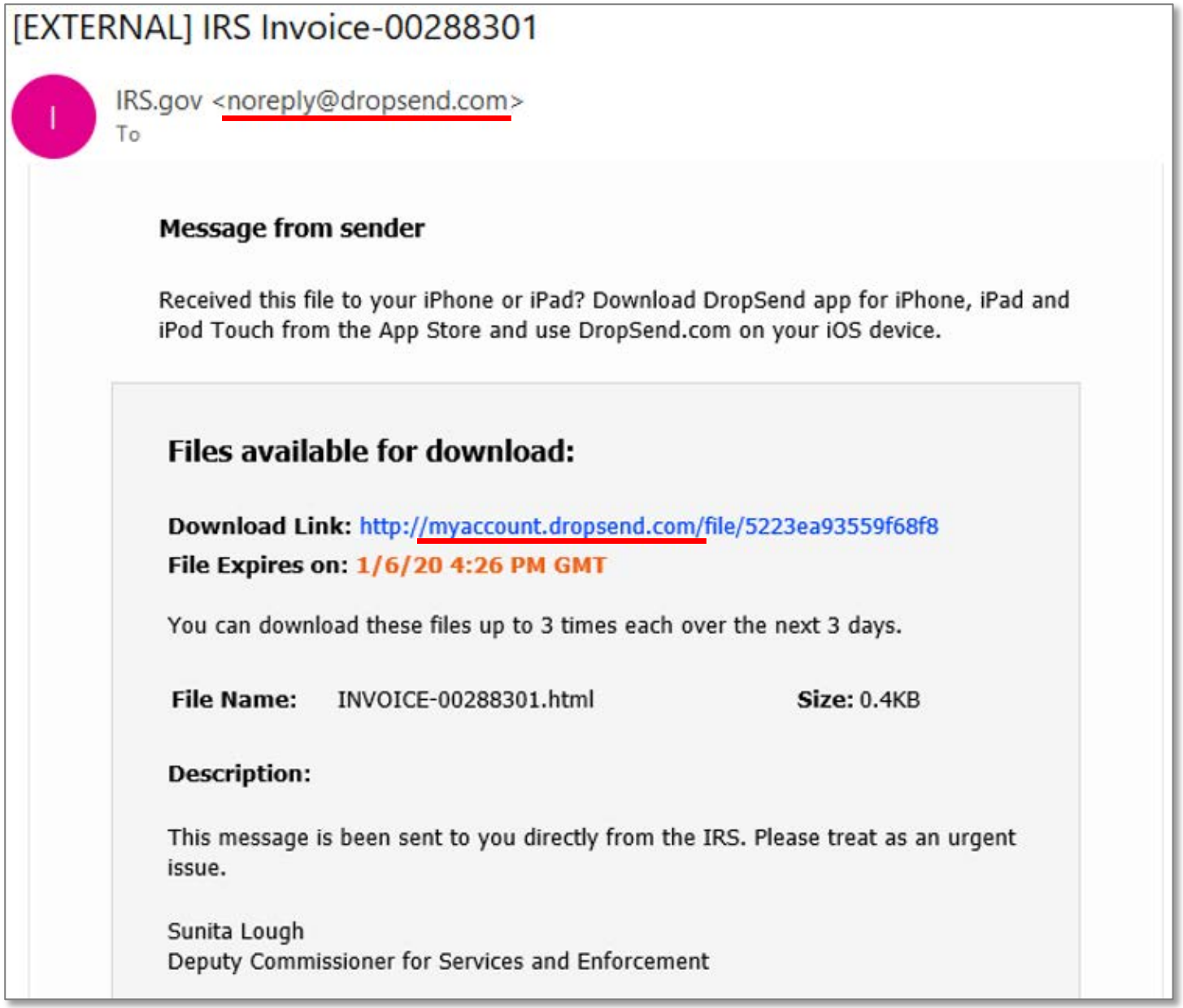
Greed	Curiosity	Self Interest
Urgency	Fear	Helpfulness

Agenda

- What is BEC?
- Tax themed attack types
- Common targets within your organization
- Defending against the attacks

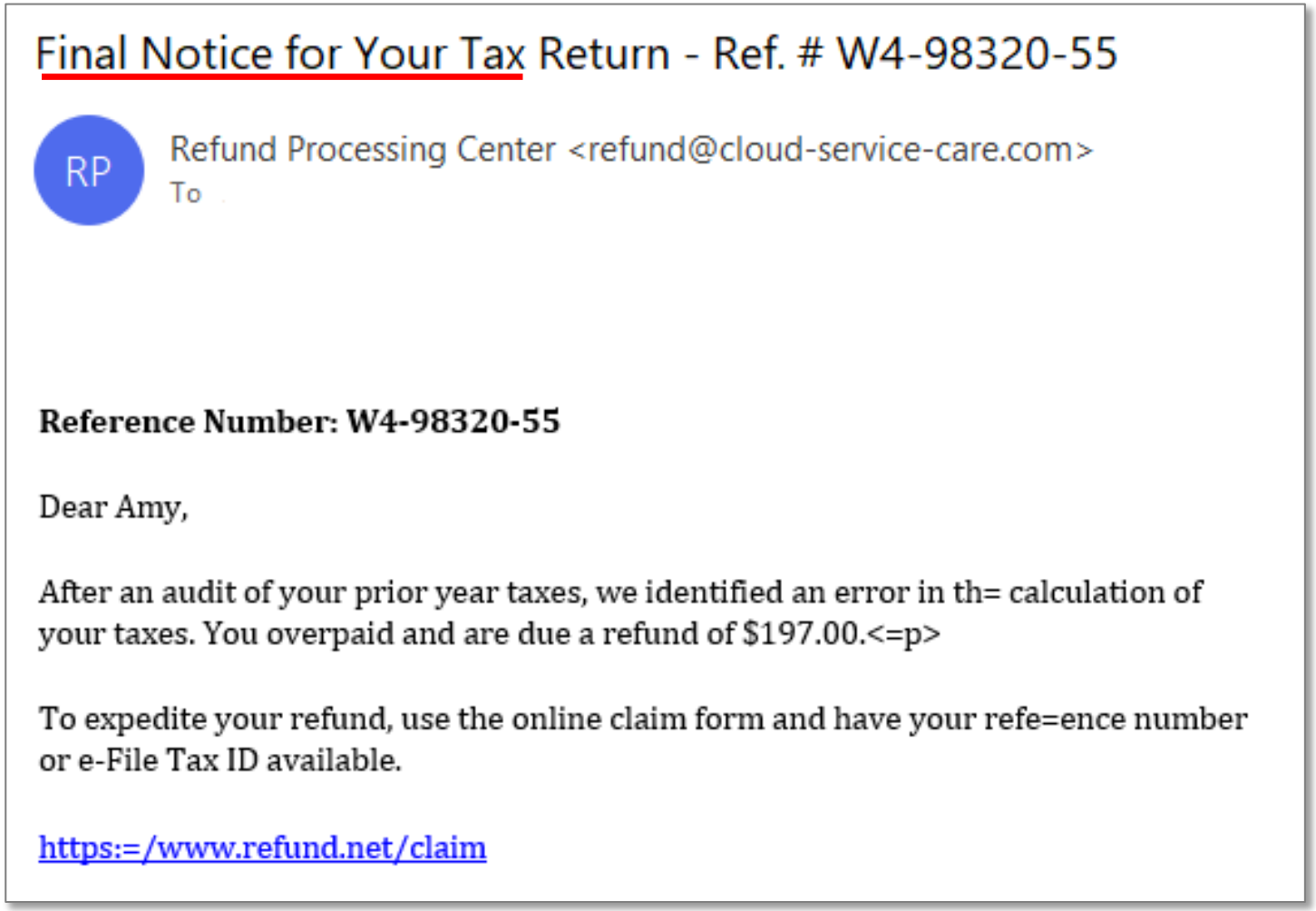
IRS Invoices

- Link with required file to download
- Using curiosity to get user to click on link
- Fear of losing file due to short time frame to download
- Noreply email address



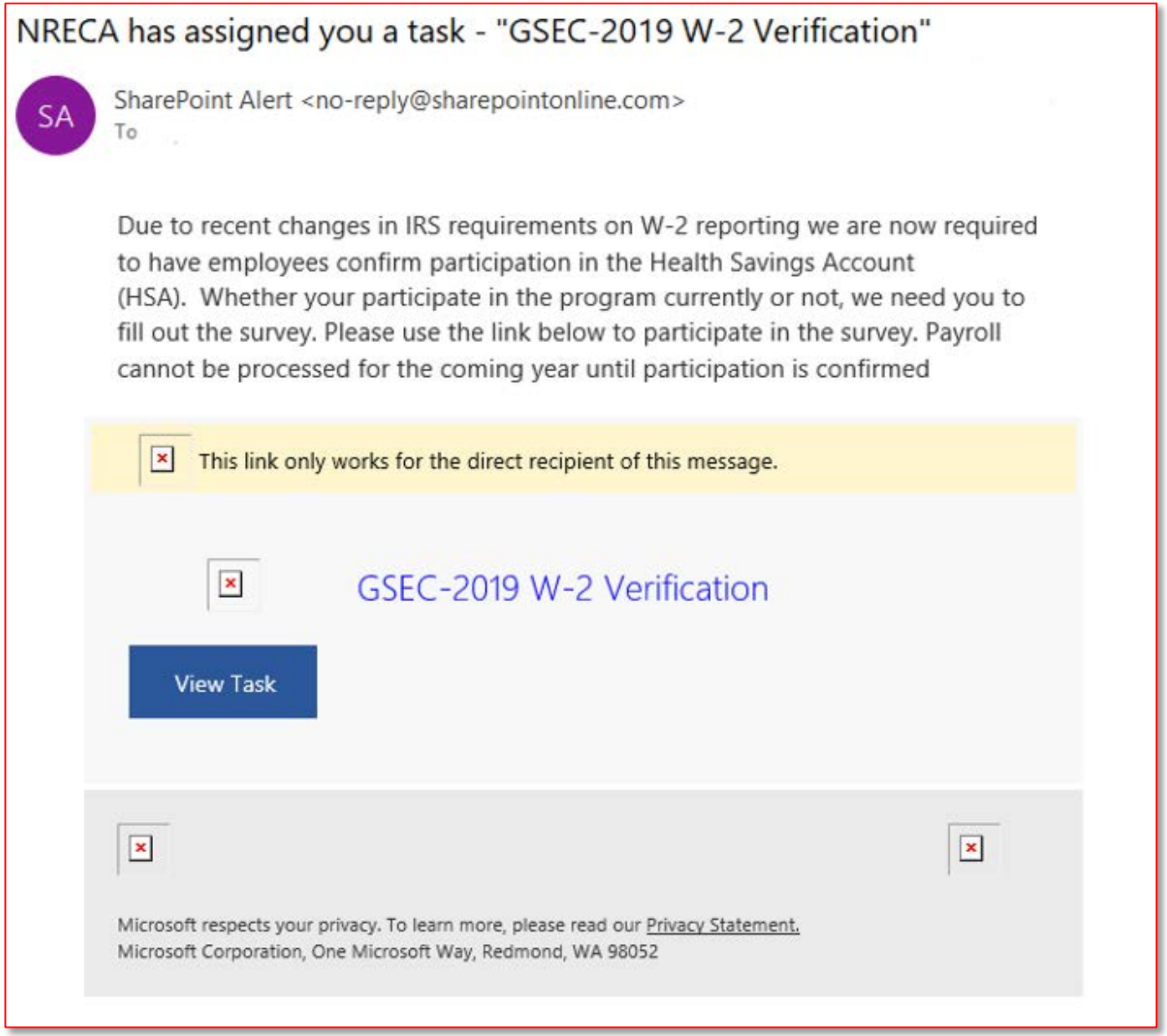
IRS Refund

- Fear of the final notice
- Audits scare people
- Refund = money for you!
- Curiosity to click the link and get money back



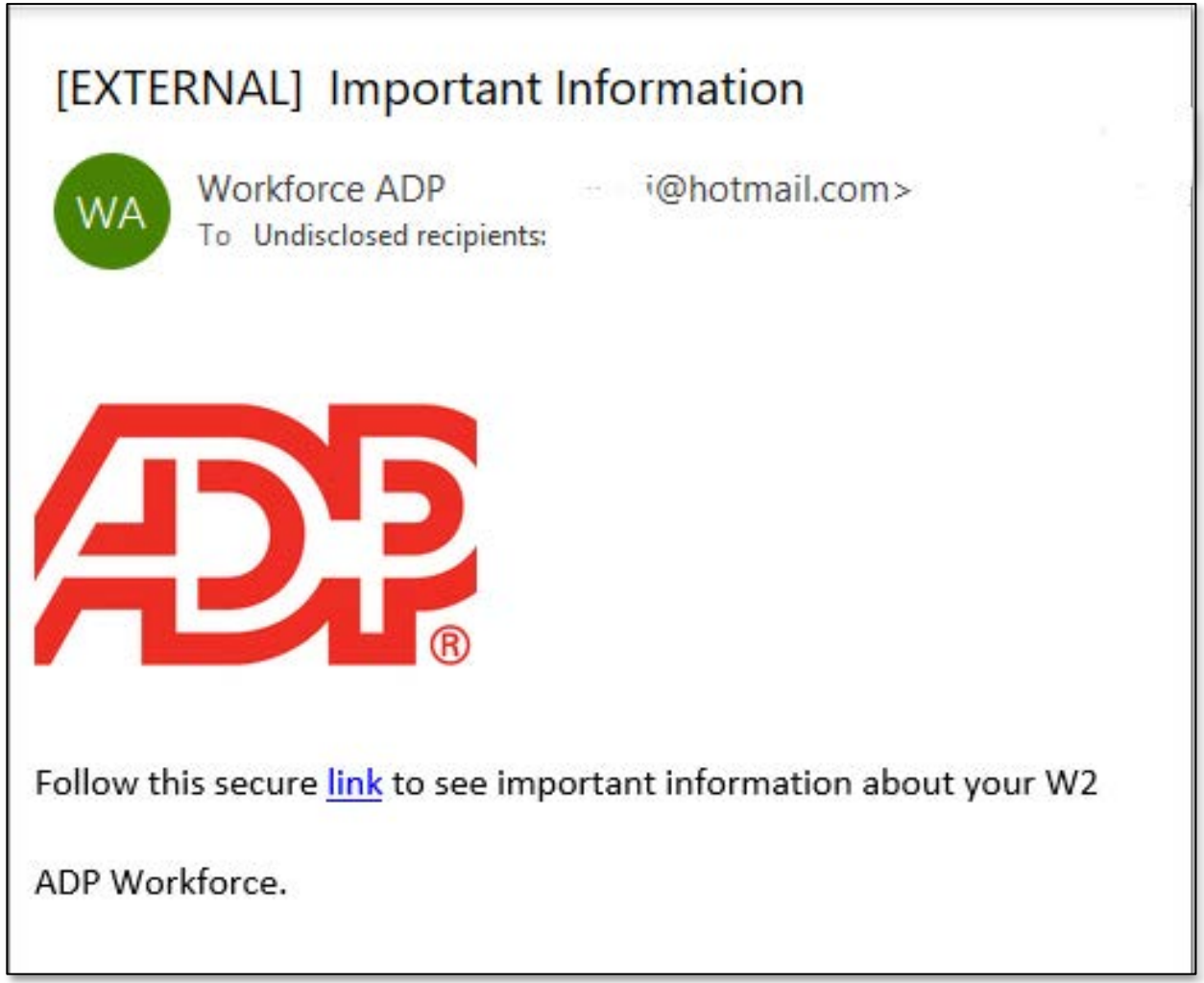
W2 Verification

- Urgency to complete form
- HSA relates to money
- Compliance to IRS, to government



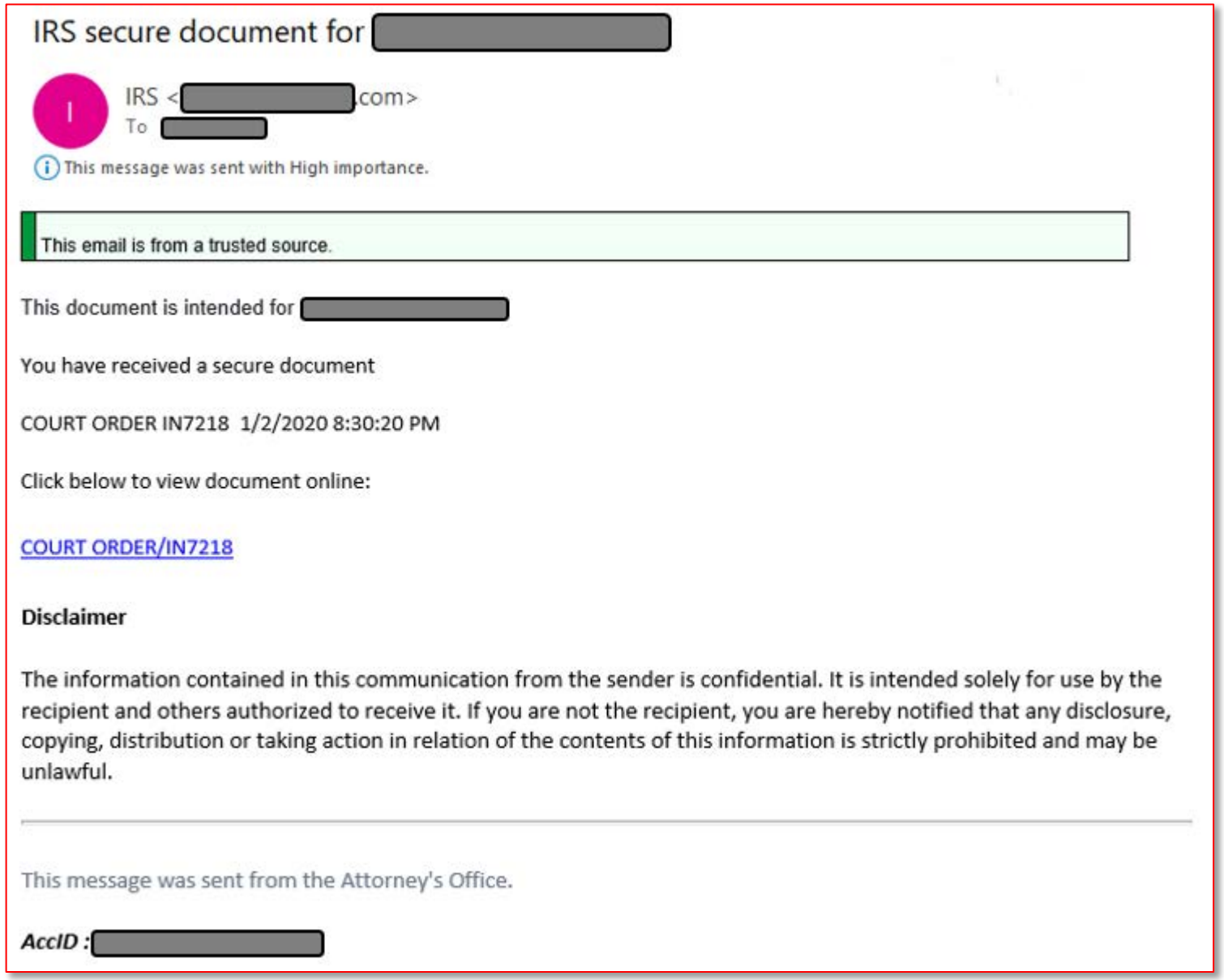
W2 Verification

- Uses a well-known vendor
- W2 information is expected at this time of year.
- Simple and to the point



IRS Court Order

- Compliance to IRS, government
- Curiosity to see the document
- Click the link to see it



IRS secure document for [redacted]

IRS <[redacted]com>
To [redacted]

This message was sent with High importance.

This email is from a trusted source.

This document is intended for [redacted]

You have received a secure document

COURT ORDER IN7218 1/2/2020 8:30:20 PM

Click below to view document online:

COURT ORDER/IN7218

Disclaimer

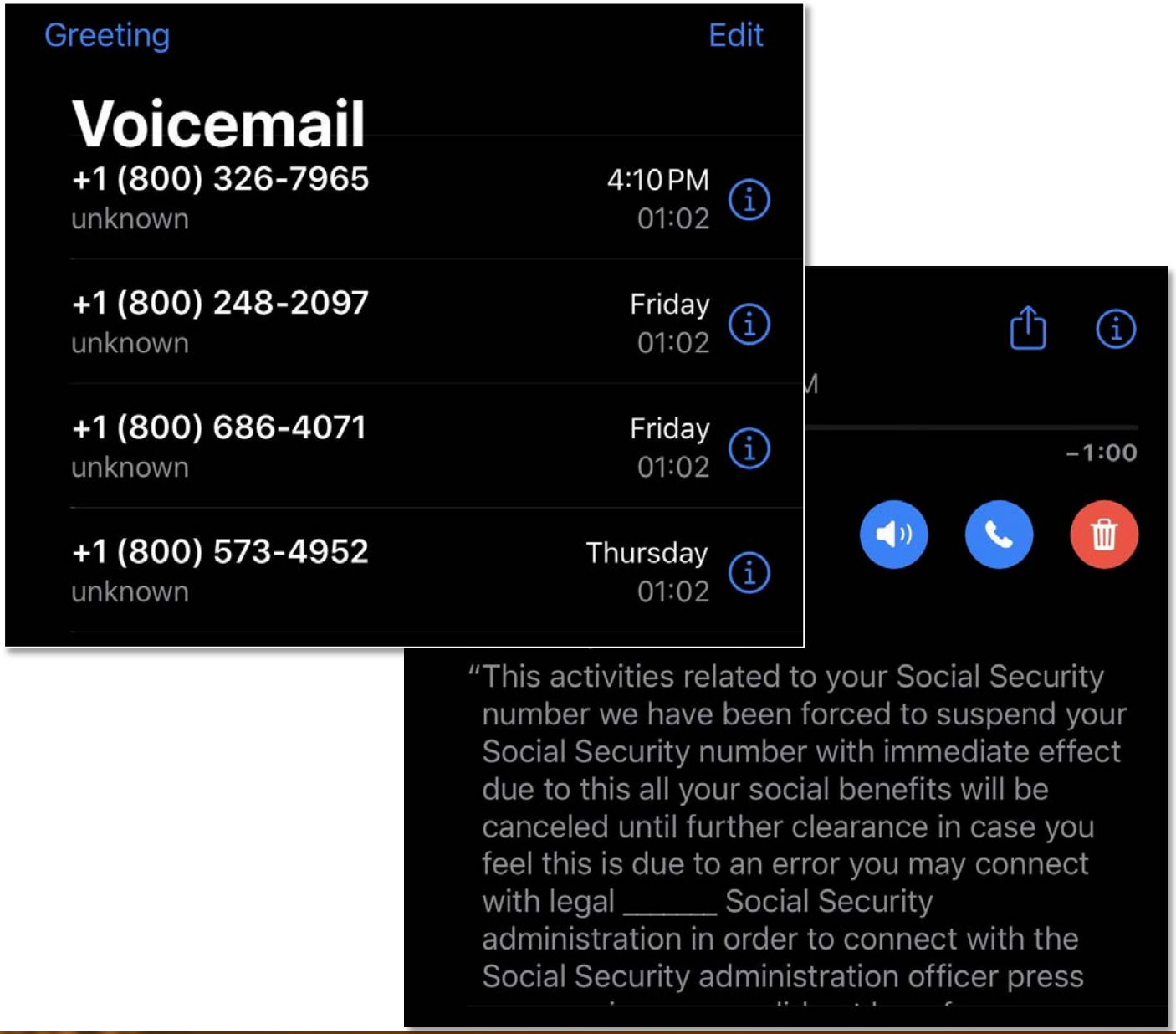
The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful.

This message was sent from the Attorney's Office.

AccID : [redacted]

SSN phone calls

- Robocalls stating your SSN is suspended have been really picking up lately.
- These often come from your local area code or from an 800 number.
- There are people waiting to speak with you personally



Agenda

- What is BEC?
- Tax themed attack types
- Common targets within your organization
- Defending against the attacks

Common Targets

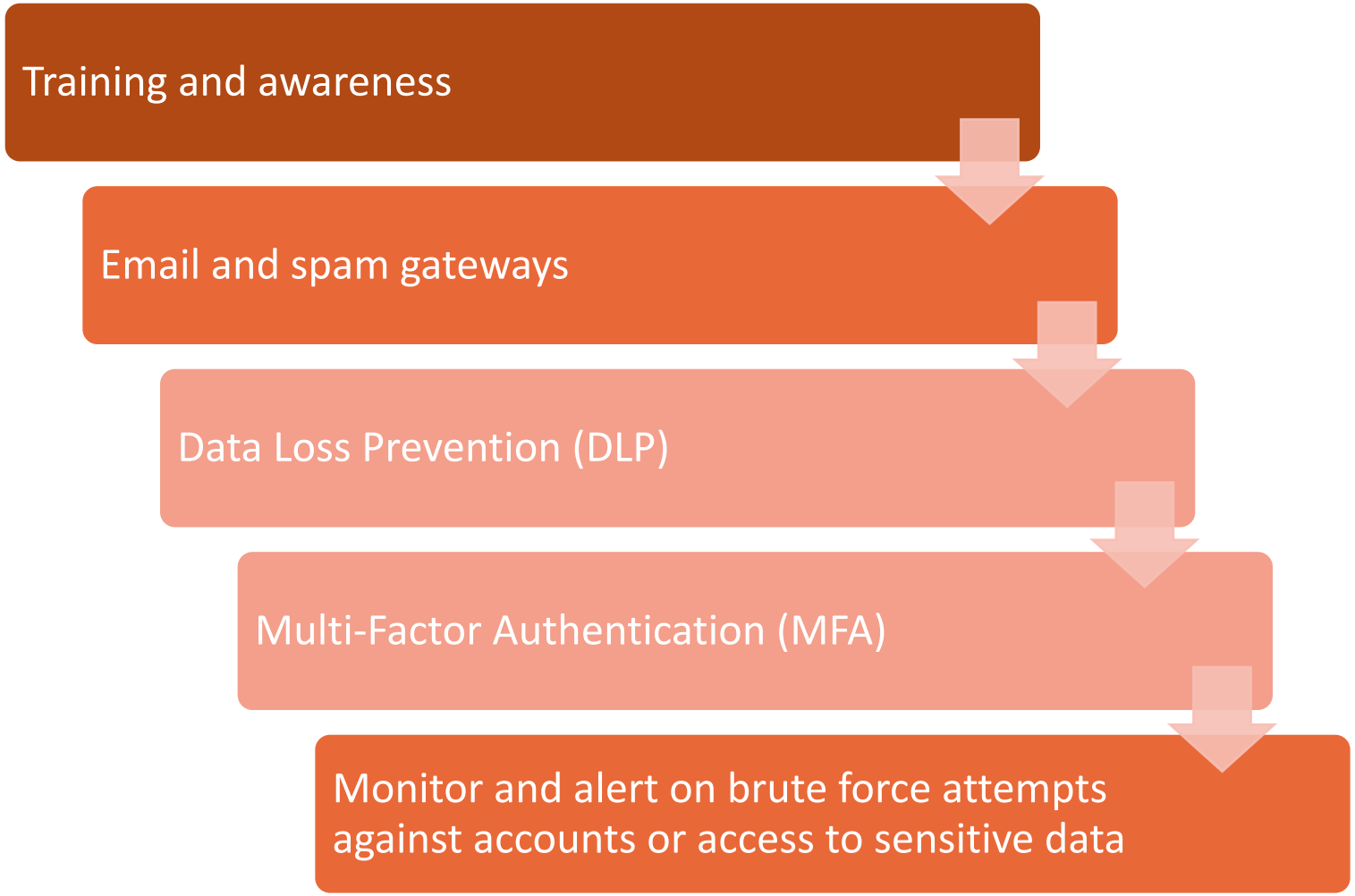
- While anyone with an email address can be a target, attackers can go after some specific people they consider “high value”
  - Executives (CEO, CFO, COO)
  - Executive Assistants
  - HR professionals
  - Payroll or Finance professionals
- They want to target people with authority and access to information and money

Agenda

- What is BEC?
- Tax themed attack types
- Common targets within your organization
- Defending against the attacks

A Layered Approach

- We know there is no silver bullet to combat any kind of insider threat, it takes layers
- Training's impact is often underestimated, and the method misunderstood



Focus on changing behavior, not just teaching a single lesson

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

Train Your Users
On-demand, interactive, engaging training with common traps, live hacking demos and new scenario-based Danger Zone exercises and educate with ongoing security hints and tips emails.

Phish Your Users
Fully automated simulated phishing attacks, hundreds of templates with unlimited usage, and community phishing templates.

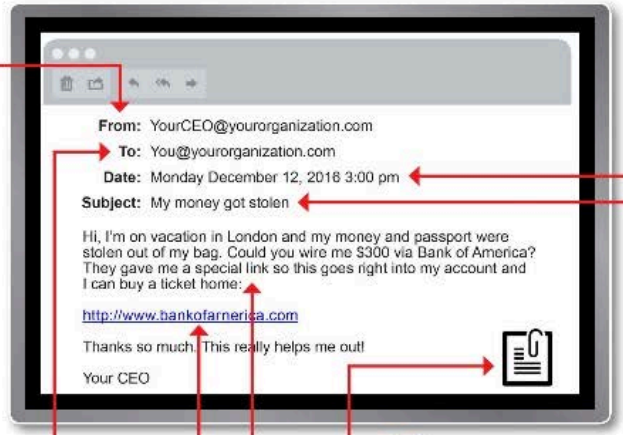
See the Results
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!


FAKE LIFE.
REAL CONSEQUENCES.
THE INSIDE MAN
KnowBe4
Human error. Conquered.
TWIST&SHOUT

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.



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**?

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.

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.

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."

CONTENT

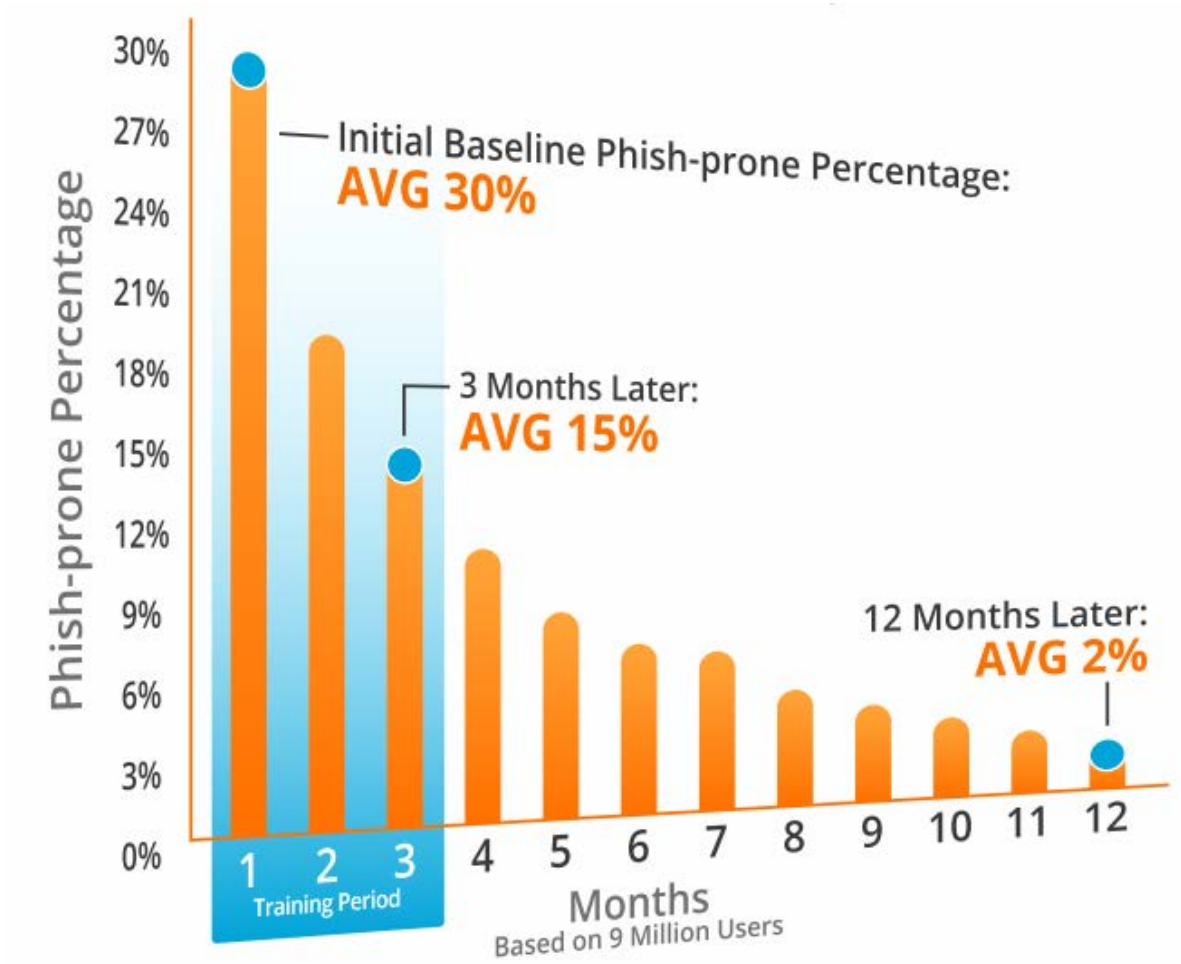
- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment 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?

KnowBe4
Human error. Conquered.

Arm Your Organization

Through combined security awareness and behavior training

Security awareness, coupled with frequent simulated phishing training, will help employees make smarter security decisions, everyday



KnowBe4
Human error. Conquered.

Thank You!

Erich Kron – Security Awareness Advocate
ErichK@KnowBe4.com | @KB4Erich | @ErichKron

James R. McQuiggan – Security Awareness Advocate
jmcquiggan@knowbe4.com | @james_mcquiggan

KnowBe4
Human error. Conquered.

Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com