KnowBe4
Human error. Conquered.

Latest Business Email Compromise Scams - Don't Be the Next Victim

Erich Kron
Security Awareness Advocate,
KnowBe4, Inc.

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.

Over

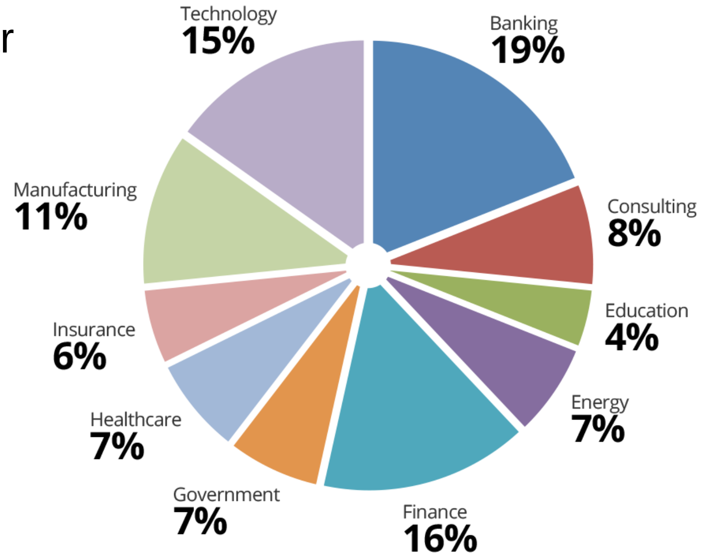
19,000

Customers

Inc. 500

About Us

- 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
- Former Gartner Research Analyst, Perry Carpenter is our Chief Evangelist and Strategy Officer
- 300% growth year over year
- We help thousands of organizations manage the problem of social engineering



Agenda

- The numbers behind the phishing problem
- The psychology behind these attacks
- Types of Business Email Compromise (BEC) attacks
- How we can defend ourselves and our organizations

Agenda

- The numbers behind the phishing problem
- The psychology behind these attacks
- Types of Business Email Compromise (BEC) attacks
- How we can defend ourselves and our organizations

Let’s Look At Phishing

KnowBe4
Human error. Conquered.

A staggering

91%

of successful data breaches started with a spear phishing attack

KnowBe4
Human error. Conquered.

Users Are The Last Line Of Defense

- **91%** of successful data breaches started with a spear phishing attack
- **CEO Fraud** (aka Business Email Compromise) causes $5.3 billion in damages
- **W-2 Scams** social engineer Accounting/HR to send tax forms to the bad guys
- **Ransomware** was a 1 Billion dollar criminal business in 2016, and continues to grow

CEO Fraud Causes $9 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 131 countries.
- Trend Micro estimates losses to exceed $9 billion in 2018.
- Between January 2015 and December 2016, there was a 2,370% increase in identified losses.

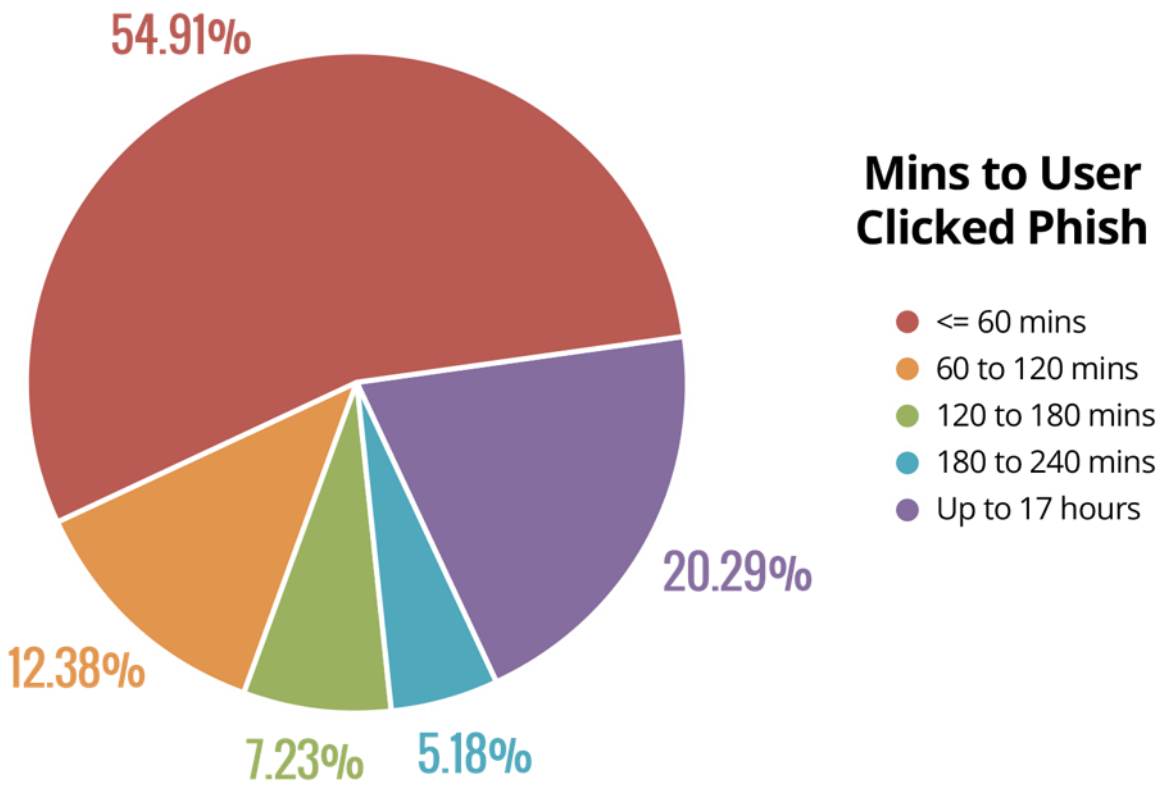
Recent studies show that over

54.9%

of users click on a phishing link in under 60 minutes

KnowBe4
Human error. Conquered.

When Do People Click On Phishing Links?



Benchmark Phish Prone Percentage by Industry

Baseline Phish Prone Percentage (B-PPP)			
Industry	**1 – 249 employees**	**250 – 999 employees**	**1000+ employees**
Energy & Utilities	31.56	29.34	22.77
Financial Services	27.41	28.47	23.00
Business Services	29.80	31.01	19.40
Technology	30.68	30.67	28.92
Manufacturing	33.21	31.06	28.71
Government	29.32	25.12	20.84
Healthcare & Pharmaceuticals	29.80	27.85	25.60
Insurance	35.46	33.32	29.19
Not For Profit	32.63	25.94	30.97
Education	29.20	26.23	26.05
Retail & Wholesale	31.58	30.91	21.93
Other	30.41	28.90	22.85

27%

Avg. Initial Baseline PPP

across all industries and sizes

Average PPP by Size of Organization

Org Size	Initial PPP
1 - 249	30.1 %
250 - 999	28.5 %
1000+	25.06 %

TOP 10 GENERAL EMAIL SUBJECTS

Password Check Required Immediately	15%
Security Alert	12%
Change of Password Required Immediately	11%
A Delivery Attempt was made	10%
Urgent press release to all employees	10%
De-activation of [[email]] in Process	10%
Revised Vacation & Sick Time Policy	9%
UPS Label Delivery, 1ZBE312TNY00015011	9%
Staff Review 2017	7%
Company Policies-Updates to our Fraternization Policy	7%

KnowBe4
Human error. Conquered.

COMMON *"IN THE WILD"* ATTACKS

- Microsoft: Re: Important Email Backup Failed
- Microsoft/Office 365: Re: Clutter Highlight
- Wells Fargo: Your Wells Fargo contact information has been updated
- Chase: Fraudulent Activity On Your Checking Account - Act Now
- Office 365: Change Your Password Immediately
- Amazon: We tried to deliver your package today
- Amazon: Refund - Valid Billing Information Needed
- IT: Ransomware Scan
- Docusign: Your Docusign account is suspended
- You have a secure message

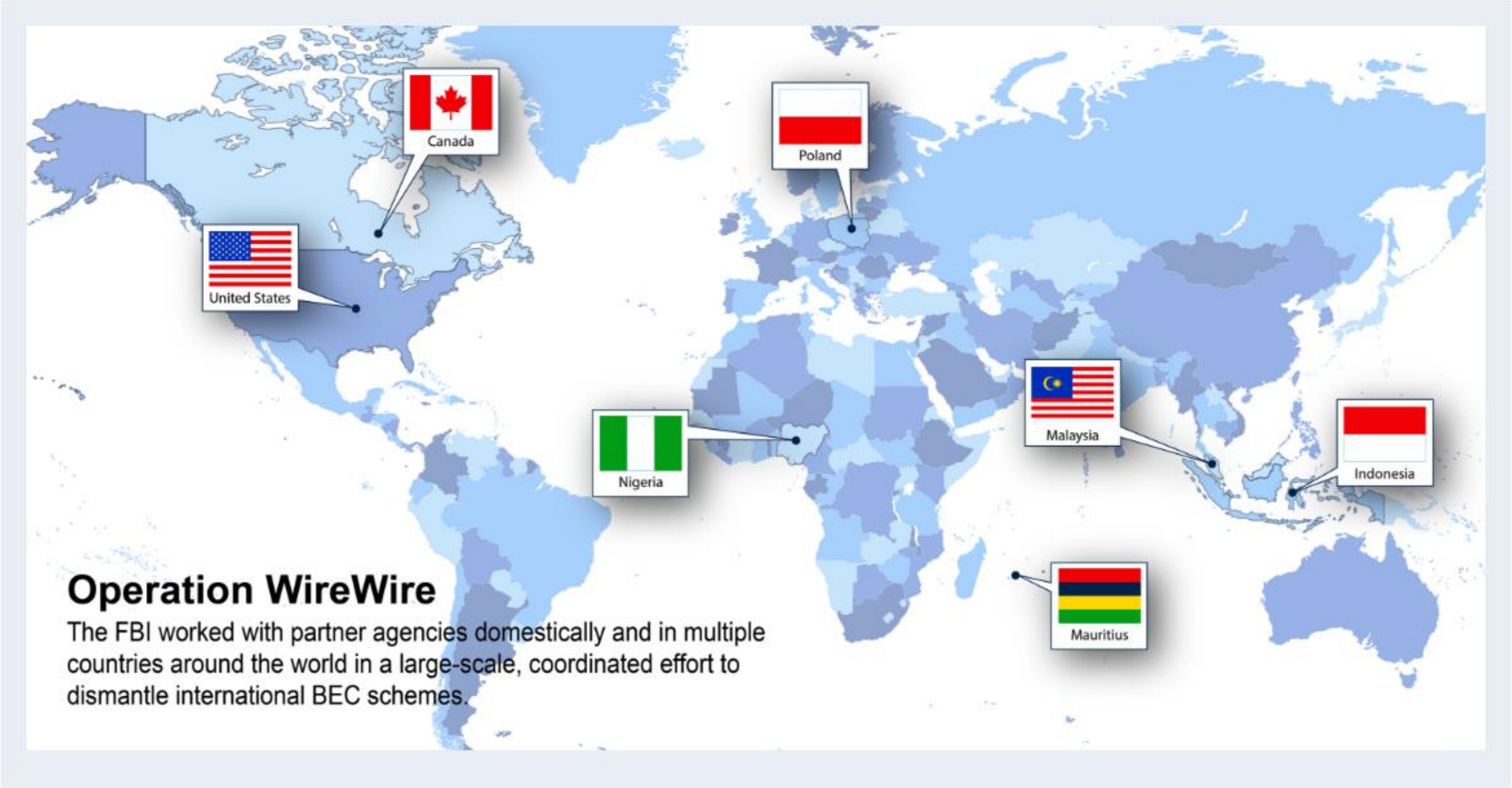
Example: Business Email Compromise (The Phish Evolved)

- a.k.a. CEO fraud, invoice fraud, payroll fraud, escrow redirection, etc.
- Often there is no payload
- Low volume email targeting high value individuals
- Personalized
- Few to no 'traditional' spam/phishing tells (such as poor grammar, egregious misspellings, etc.)

Do They Ever Get Caught?

- Not often, but it does happen. This is from June 11, 2018

- Operation WireWire Included U.S. Department of Justice, FBI, Department of Homeland Security, the Department of the Treasury, and the U.S. Postal Inspection Service
- 74 arrests
- Seizure of roughly $2.4 million
- Disrupted and recovered about $14 million in fraudulent wore transfers

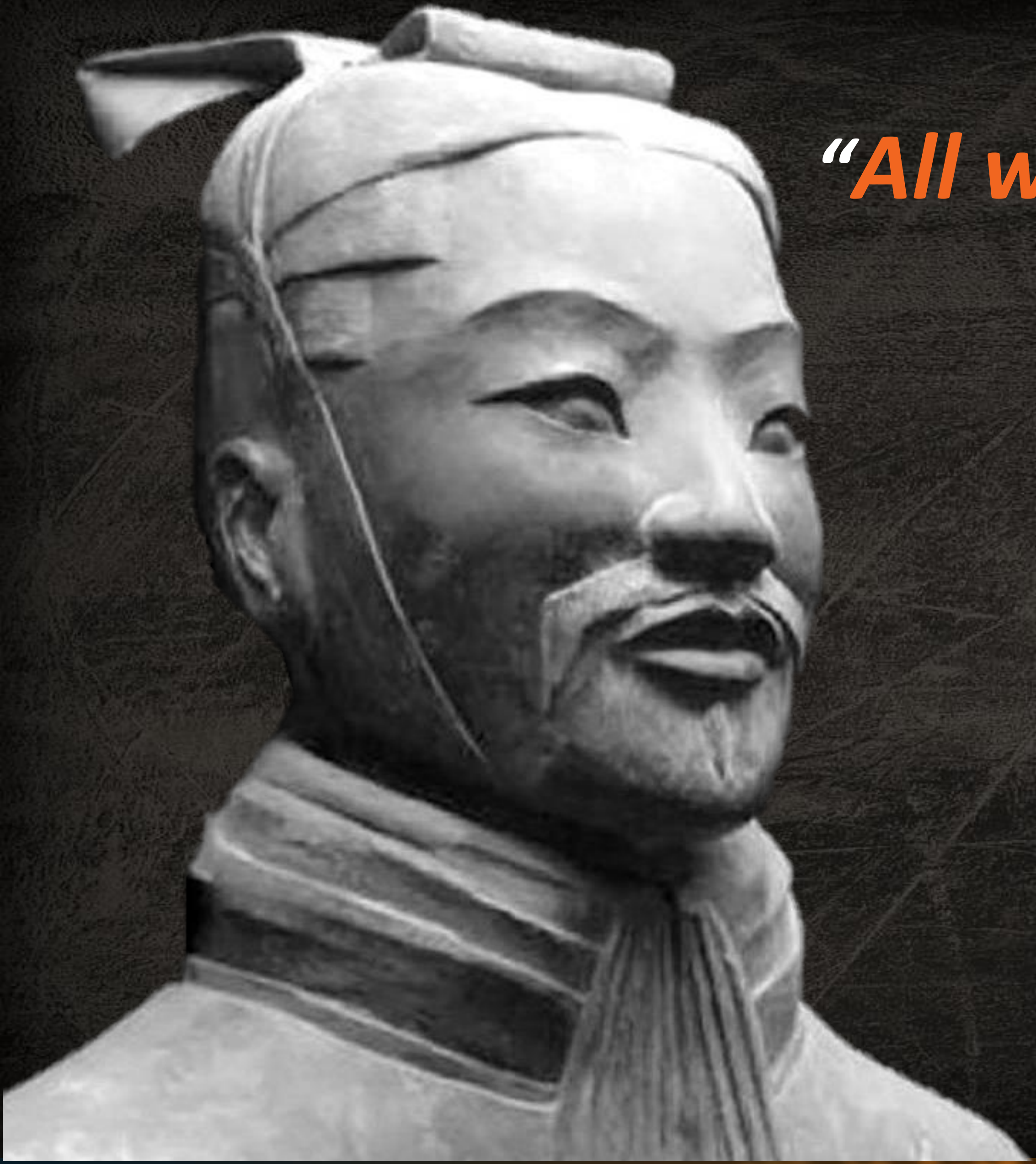


Operation WireWire

The FBI worked with partner agencies domestically and in multiple countries around the world in a large-scale, coordinated effort to dismantle international BEC schemes.

Agenda

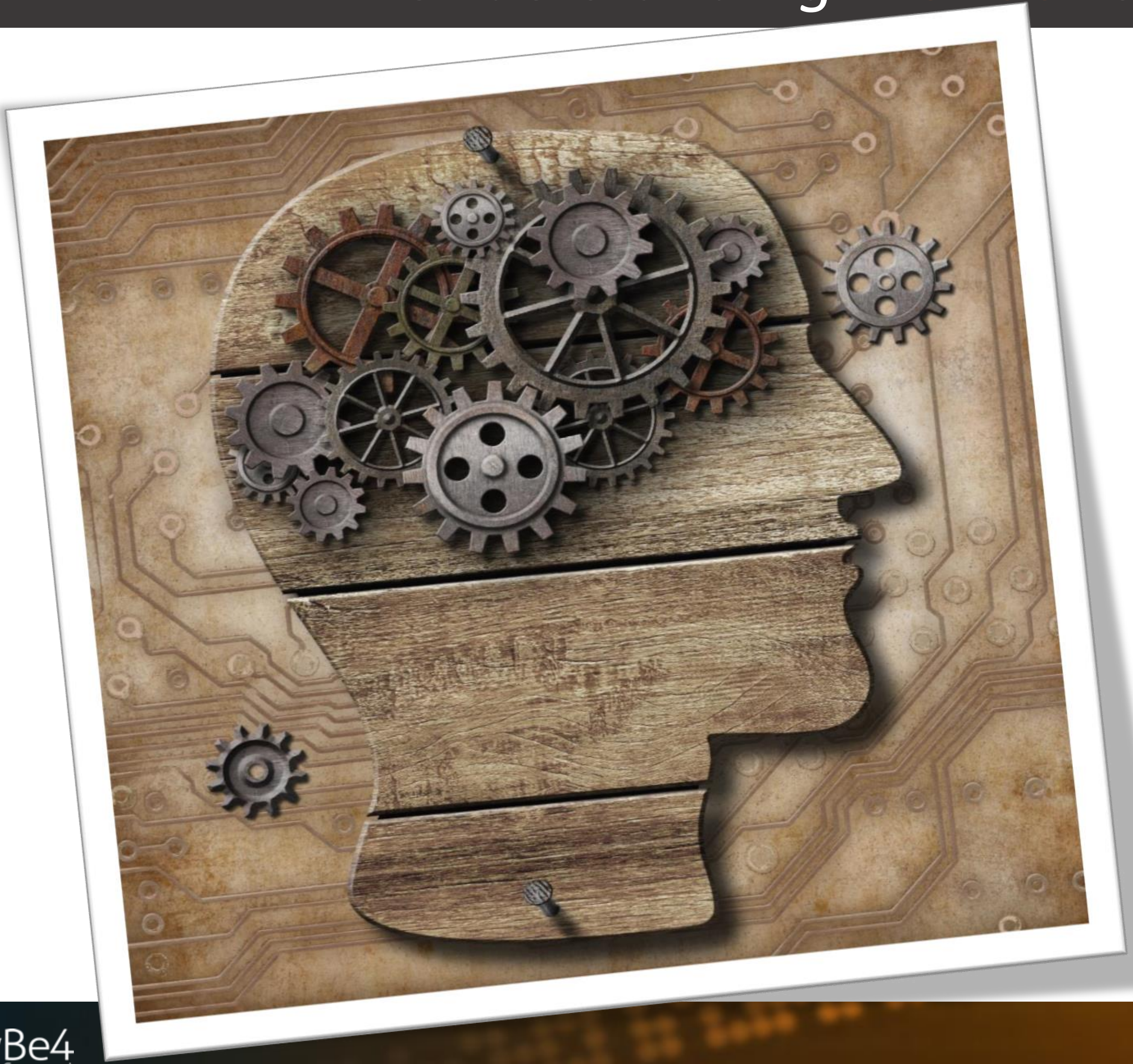
- The numbers behind the phishing problem
- The psychology behind these attacks
- Types of Business Email Compromise (BEC) attacks
- How we can defend ourselves and our organizations



“All warfare is based on deception.”

- Sun Tzu, *The Art of War*

Understanding the root of deception



Our brains' job to filter, interpret, and present 'reality'

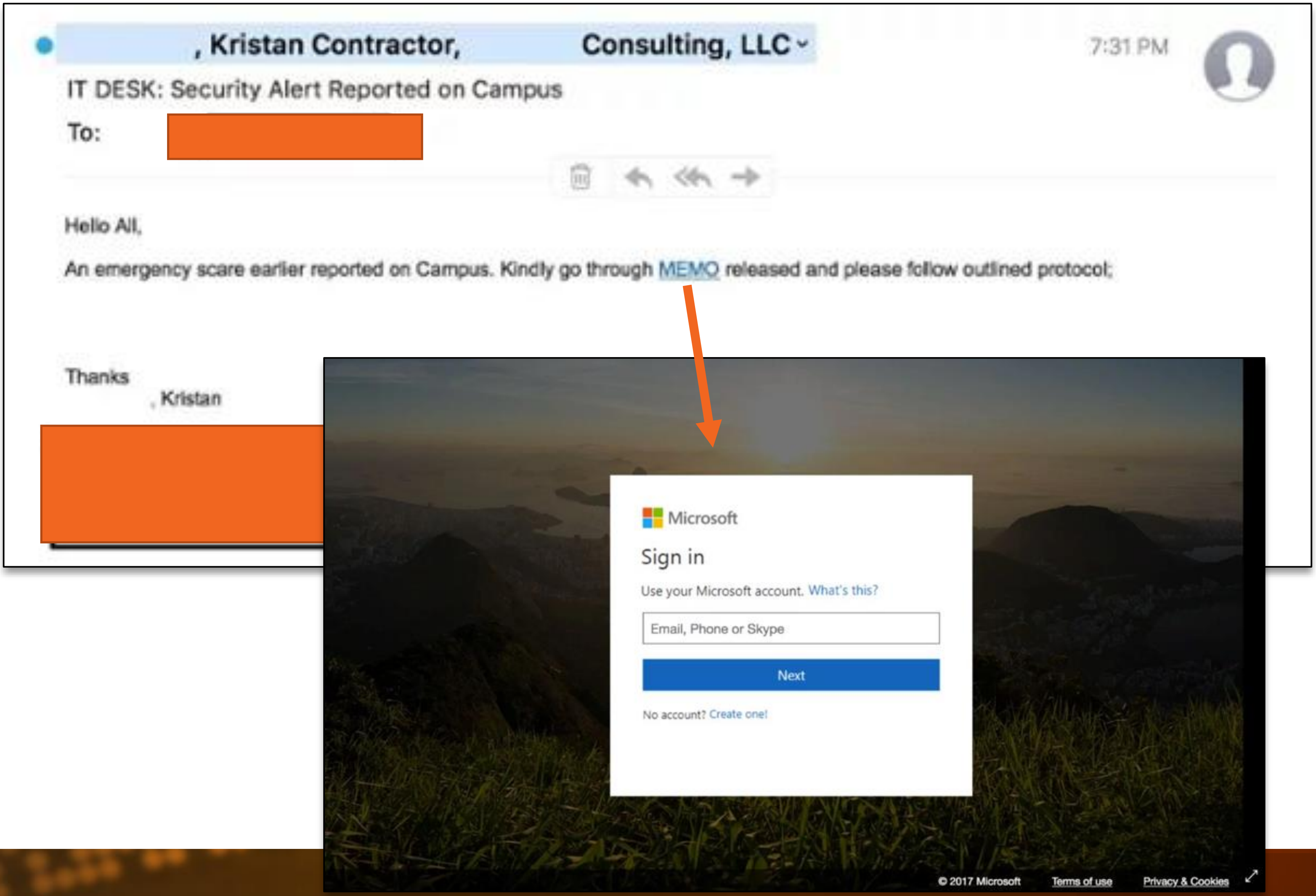
Are You Being Manipulated?

-- understand the lures --

Greed	Curiosity	Self Interest
Urgency	Fear	Helpfulness

Attackers will do *anything* to bypass critical thinking

- Spoofs a campus-wide security alert for a community college (confidential information blocked out) in Florida.
- Exploits current concerns over active shooters on education campuses
- Crafted to generate a reflexive click.
- Directs to credential capture site.
- Other variants seen:
    - "IT DESK: Security Alert Reported on Campus"
    - "IT DESK: Campus Emergency Scare"
    - "IT DESK: Security Concern on Campus Earlier"



, Kristan Contractor, Consulting, LLC 7:31 PM

IT DESK: Security Alert Reported on Campus

To: [redacted]

Hello All,

An emergency scare earlier reported on Campus. Kindly go through MEMO released and please follow outlined protocol;

Thanks
, Kristan

[redacted]

Agenda

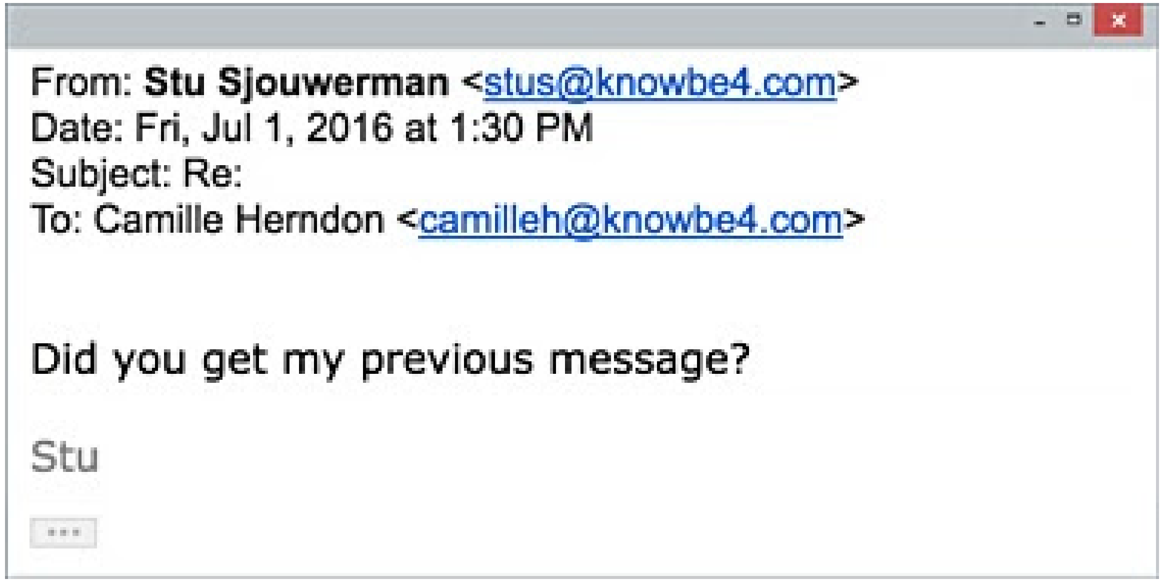
- The numbers behind the phishing problem
- The psychology behind these attacks
- Types of Business Email Compromise (BEC) attacks
- How we can defend ourselves and our organizations

Business Email Compromise Examples

- Wire transfer fraud
- W2 fraud
- Supply chain/invoice fraud
- Escrow redirection
- Payroll fraud

How CEO Fraud Plays Out

- KnowBe4 had just hired a new controller. Part of the onboarding process is updating LinkedIn
- A few weeks later, she receives this email, but the email headers proved it's not from Stu
- This was a real CEO fraud attempt, just a few weeks after she had updated her LinkedIn account



From: **Stu Sjouwerman** <stus@knowbe4.com>
Date: Fri, Jul 1, 2016 at 1:30 PM
Subject: Re:
To: Camille Herndon <camilleh@knowbe4.com>

Did you get my previous message?

Stu

...

Two Unnamed US Companies Falls Victim to $100 Million CEO Email Fraud

- This scam only surfaced as the U.S. government filed a civil forfeiture lawsuit in federal court in Manhattan seeking to recover tens of millions held in at least 20 bank accounts around the world.

- The scammer, a 48-year old Lithuanian managed to trick two American technology companies into wiring him **$100 million**.

- What makes this remarkable is the amount of money he managed to score and the industry from which he stole it. The indictment specifically describes the companies in vague terms, but Apple, Cisco, HP and Facebook come to mind.

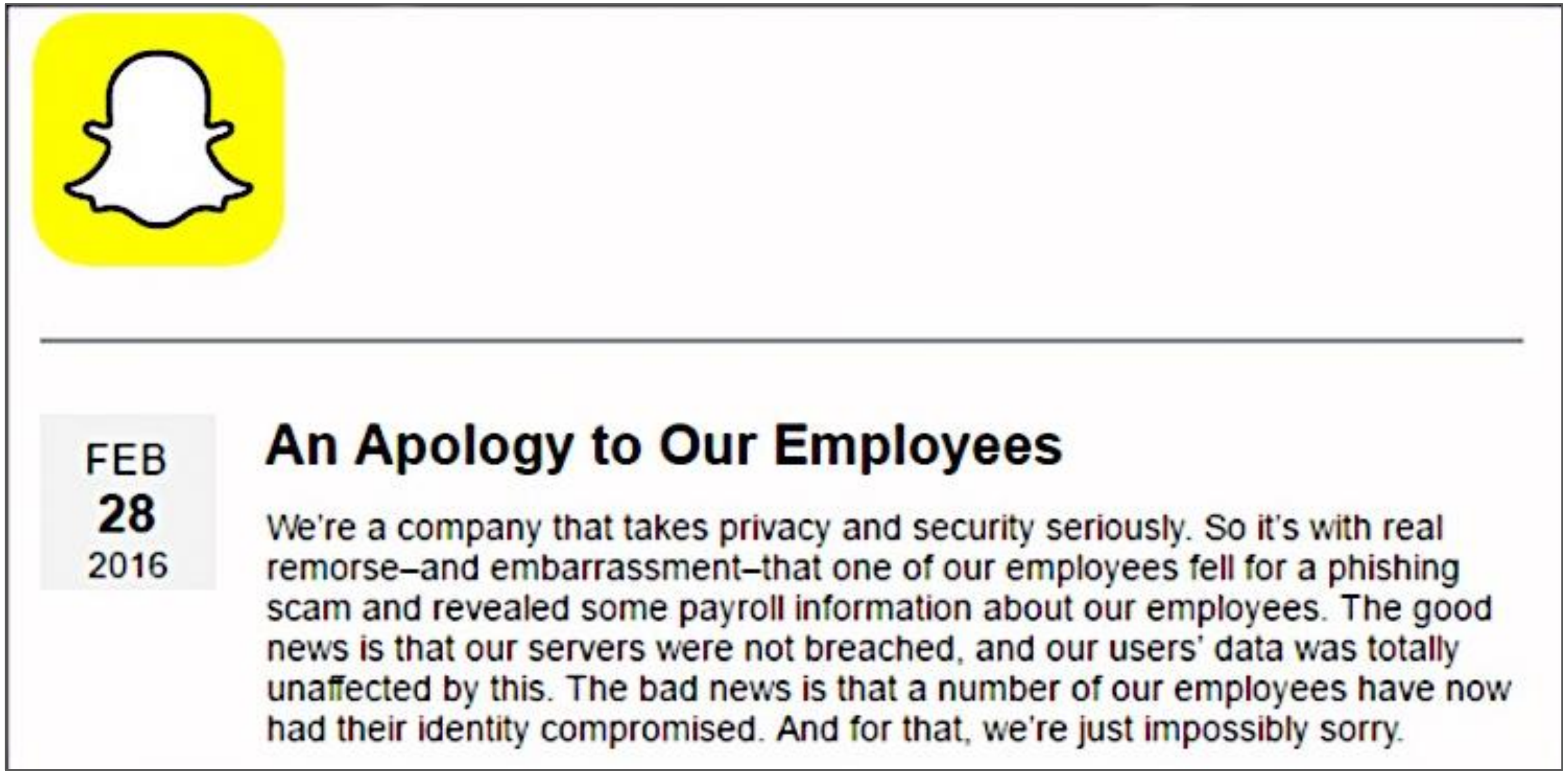
$44 Million in a Single CEO Fraud Attack

- Leoni AG fell victim to a classic CEO fraud attack that has cost the company a whopping **44 million dollars**.
- Attackers crafted emails to appear like legitimate payment requests from the head office in Germany and sent them to a subsidiary of Leoni in Bistrita, Romania.
- The scammers had extensive knowledge about the internal procedures for approving and processing transfers, meaning the network had likely been penetrated months earlier.

Business Email Compromise Examples

- Wire transfer fraud
- W2 fraud
- Supply chain/invoice fraud
- Escrow redirection
- Payroll fraud

W2 Scam Hits SnapChat

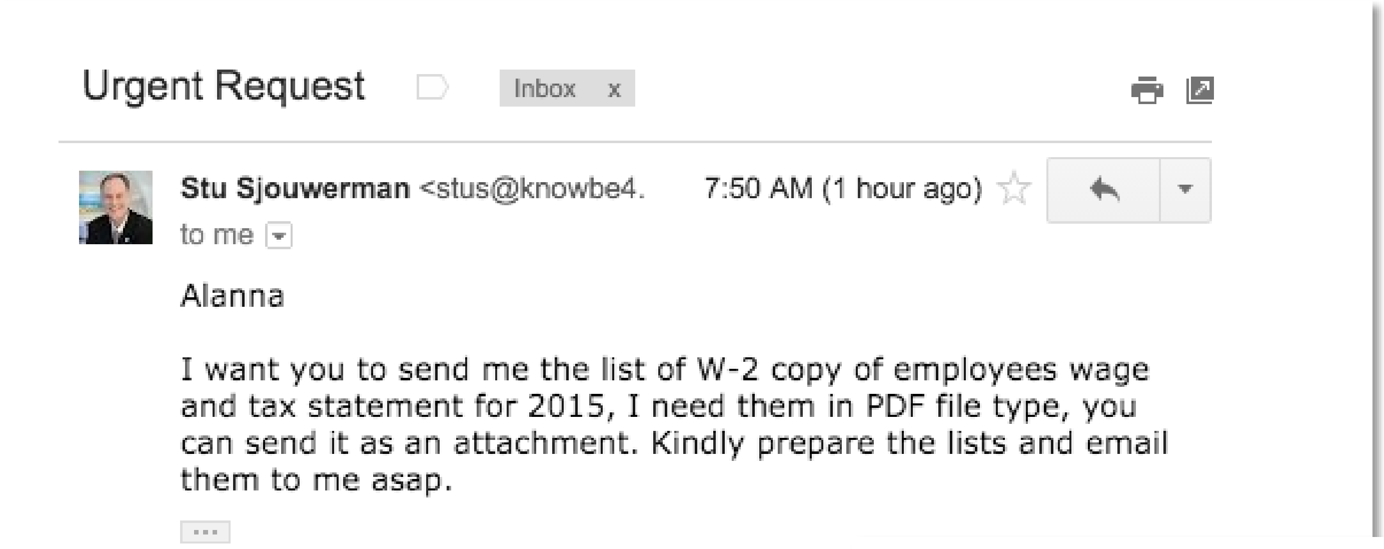


FEB
28
2016

An Apology to Our Employees

We're a company that takes privacy and security seriously. So it's with real remorse–and embarrassment–that one of our employees fell for a phishing scam and revealed some payroll information about our employees. The good news is that our servers were not breached, and our users' data was totally unaffected by this. The bad news is that a number of our employees have now had their identity compromised. And for that, we're just impossibly sorry.

Right Here at KnowBe4



Urgent Request

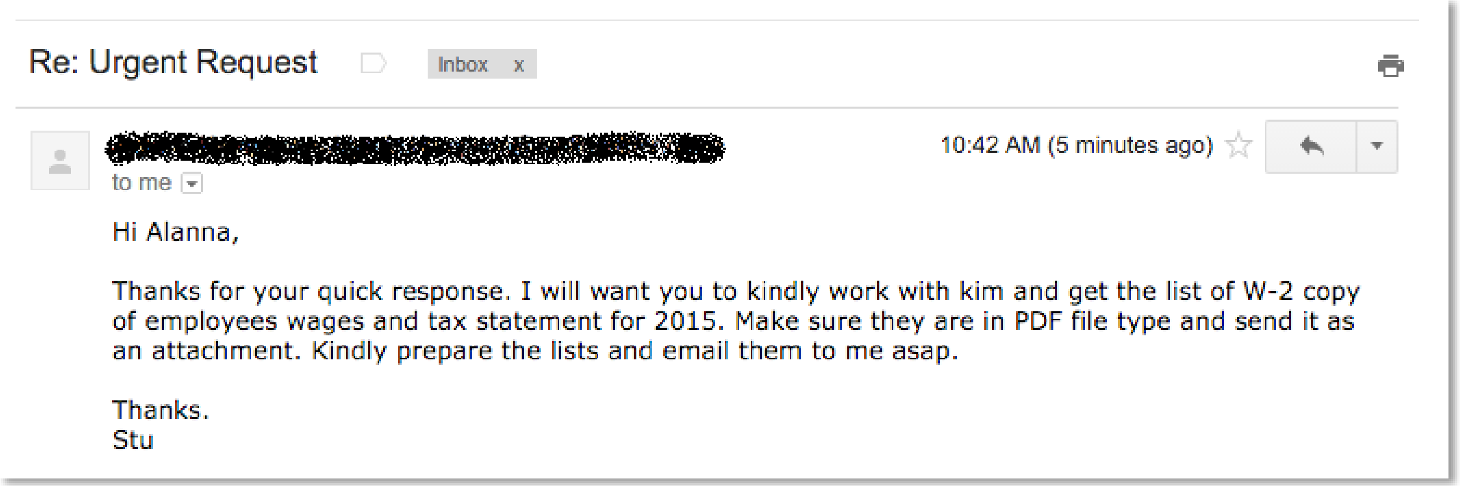
Stu Sjouwerman <stus@knowbe4.

7:50 AM (1 hour ago)

to me

Alanna

I want you to send me the list of W-2 copy of employees wage and tax statement for 2015, I need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me asap.



Re: Urgent Request

[redacted]

10:42 AM (5 minutes ago)

to me

Hi Alanna,

Thanks for your quick response. I will want you to kindly work with kim and get the list of W-2 copy of employees wages and tax statement for 2015. Make sure they are in PDF file type and send it as an attachment. Kindly prepare the lists and email them to me asap.

Thanks.
Stu

My W-2 Fraud Story

- 250 employee company
- Not really well known or heavily marketed
- President was traveling, the email requested W-2s
- Signature was correct, probably from his out-of-office reply

- HR person felt something was fishy (phishy?) and gave me a call

Business Email Compromise Examples

- Wire transfer fraud
- W2 fraud
- Supply chain/invoice fraud
- Escrow redirection
- Payroll fraud

Supply Chain and Invoice Fraud

- Criminals gain access to an email account and monitor incoming and outgoing emails.

- When the person with the compromised email account sends an invoice to a client via email, the attackers immediately send a duplicate, fraudulent invoice from the same email address, telling the client the made a mistake and to wire money to the account in the revised invoice.

- Attackers may also just generate fake invoices and send them to clients, which they are able to identify from previous email conversations.

Business Email Compromise Examples

- Wire transfer fraud
- W2 fraud
- Supply chain/invoice fraud
- Escrow redirection
- Payroll fraud

Escrow Redirection

- Very similar to invoice fraud.
- Criminals gain access to an email account and monitor incoming and outgoing emails.
- When the person with the compromised email account sends a request to transfer escrow funds via email, the attackers immediately send a duplicate, fraudulent email from the same email address, telling the client the made a mistake and to wire money to a different account.

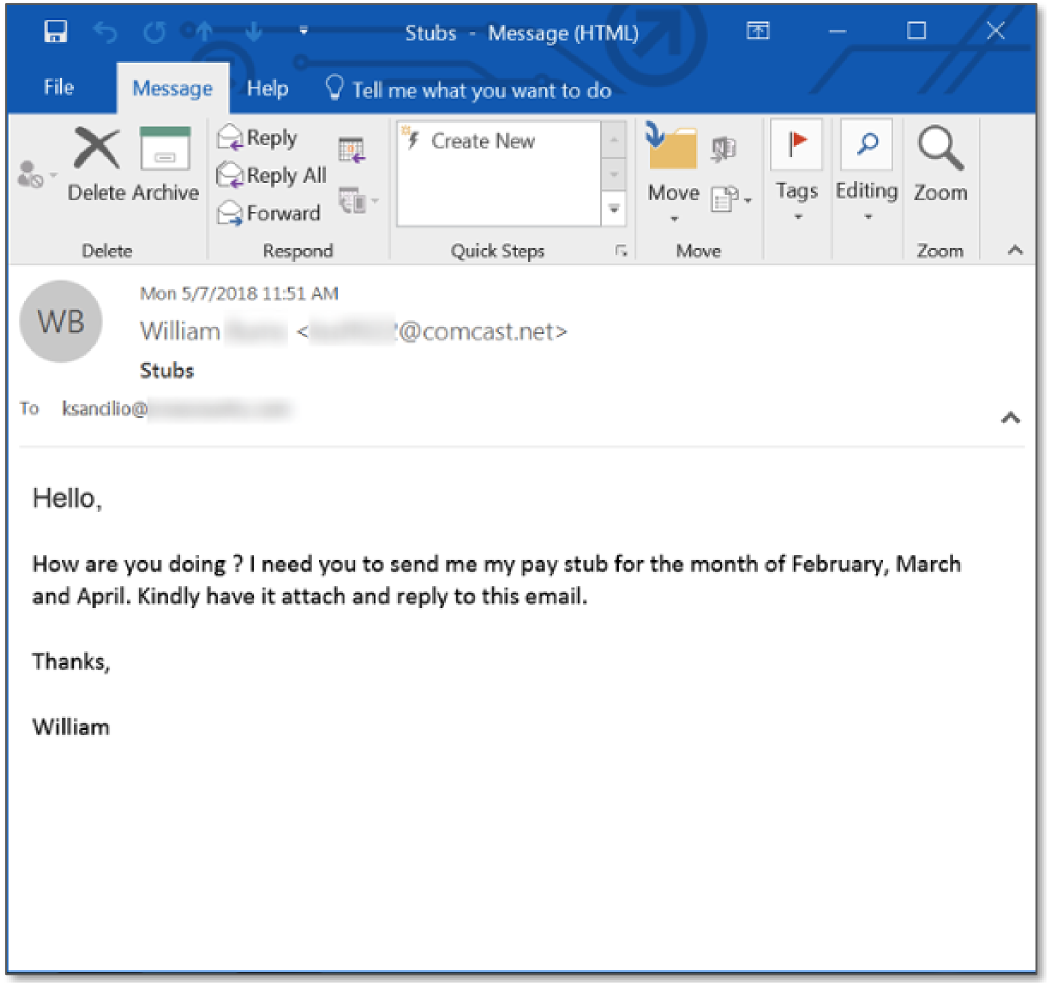
Business Email Compromise Examples

- Wire transfer fraud
- W2 fraud
- Supply chain/invoice fraud
- Escrow redirection
- Payroll fraud

Payroll Fraud

Pay Stub Phishes

- Similar to W2 fraud, but much more targeted.
- Because these emails typically request a single, specific pay stub, these emails seem designed to "fly under the radar" and not attract undue attention.



Mon 5/7/2018 11:51 AM

William [redacted] <[redacted]@comcast.net>

Stubs

To ksandilio@[redacted]

Hello,

How are you doing ? I need you to send me my pay stub for the month of February, March and April. Kindly have it attach and reply to this email.

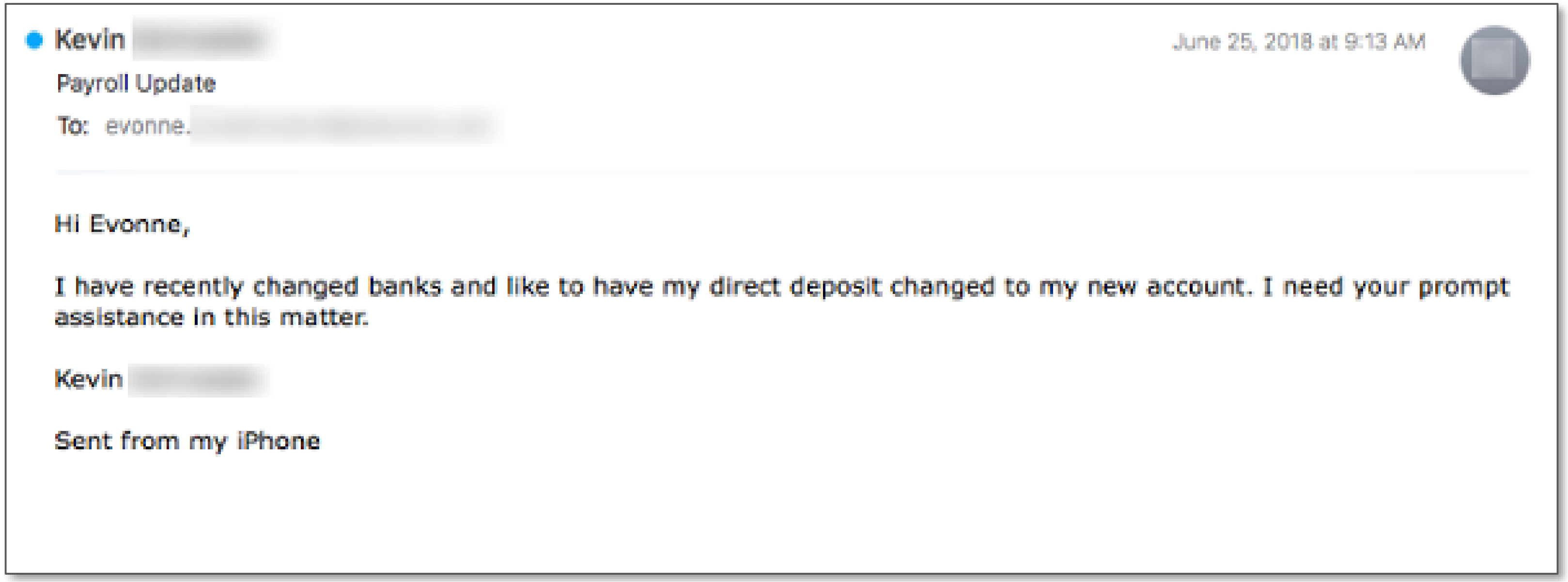
Thanks,

William

Payroll Fraud

Payroll Updates

- These go straight for the money and try to redirect a paycheck to an attackers account.
- These are simple and direct attacks



Kevin [redacted]

June 25, 2018 at 9:13 AM

Payroll Update

To: evonne.[redacted]

Hi Evonne,

I have recently changed banks and like to have my direct deposit changed to my new account. I need your prompt assistance in this matter.

Kevin [redacted]

Sent from my iPhone

Agenda

- The numbers behind the phishing problem
- The psychology behind these attacks
- Types of Business Email Compromise (BEC) attacks
- How we can defend ourselves and our organizations

Multi-Factor Authentication

- While it’s always better to avoid giving up the credentials in the first place, you can use 2-Factor (2FA) or Multi-Factor (MFA) authentication to help mitigate the risks of credential theft

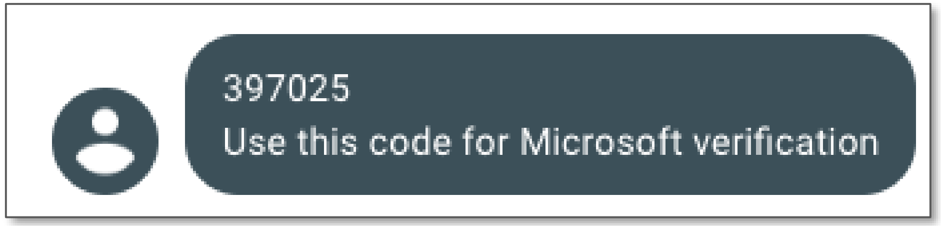
- Multi-Factor is not fool-proof and can be bypassed, however it is still more secure than a single factor

- My preference in order of security is as follows:
  - SMS-based
  - Application-based
  - Hardware-based

Multi-Factor Authentication

- SMS-based 2FA relies on a text message being sent, usually with a code, to be used in addition to the password when logging in to an account

- This is arguably the least safe, but is better than nothing and often more convenient than other methods

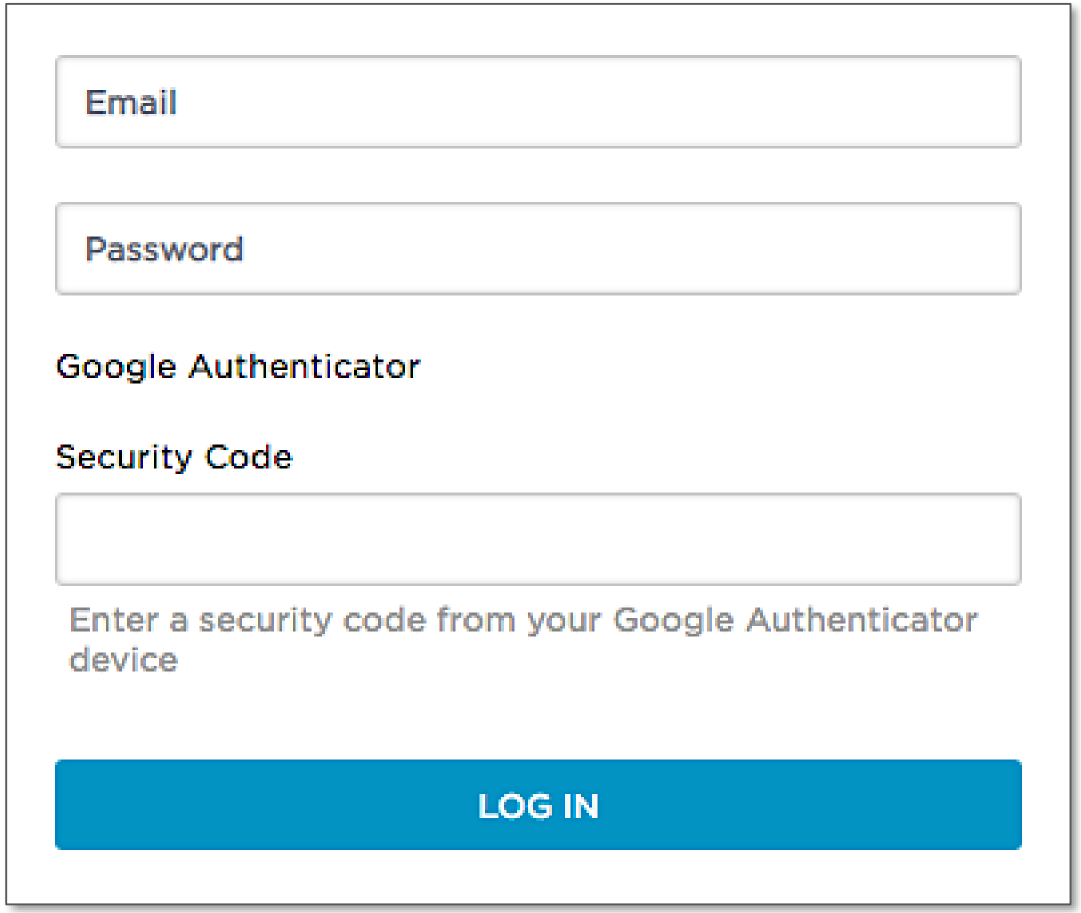


397025
Use this code for Microsoft verification

Multi-Factor Authentication

- Application-based 2FA uses an application, usually time-based and installed on a mobile device like a smart phone, to generate a code to be used in addition to the password when logging in to an account

- These codes are typically time-based and change often, usually every 60 seconds or so. This is more secure than SMS, without being much more inconvenient



Enter a security code from your Google Authenticator device

Multi-Factor Authentication

- Hardware-based 2FA uses a hardware token, like a Yubikey or Google Titan key, to be used in addition to the password while logging in to an account
- These often support FIDO U2F, One-Time-Passwords (OTP) and PIV certificate-based authentication
- These are very secure, but can be inconvenient when forgotten or damaged

Arm Employees for Battle

KnowBe4
Human error. Conquered.

Be **completely honest** with yourself about your **goals** and what your current **organizational culture** will tolerate

KnowBe4
Human error. Conquered.

Comprehensive Programs Work

- Most security awareness programs are still too superficial and done for compliance reasons
- What is missing is the correct estimation of the adversary being faced and the degree of commitment an organization has to have to stave of attacks
- Training on its own, typically once a year, isn’t enough
- Simulated phishing of groups of employees on its own doesn’t work
- But together, they can be combined to greatly increase effectiveness

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.

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."

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.

Training: How To Do It Right

KnowBe4
Human error. Conquered.

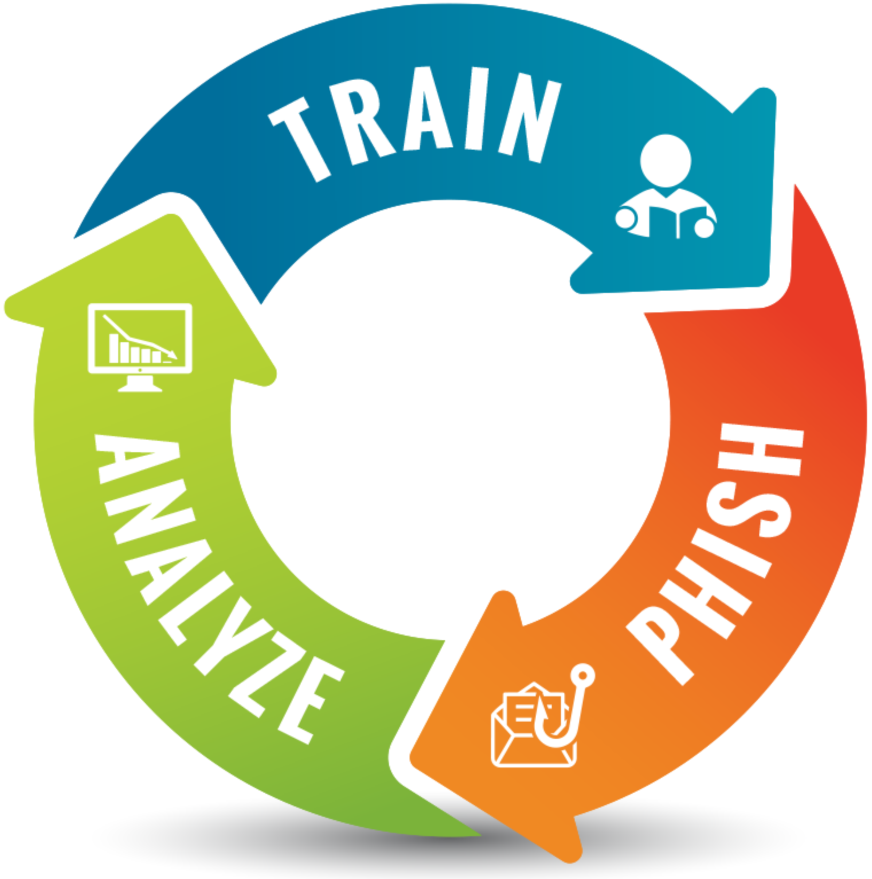
The KnowBe4 Security Awareness Program WORKS

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 Kevin Mitnick demos and new scenario-based Danger Zone exercises and educate with ongoing security hints and tips emails.

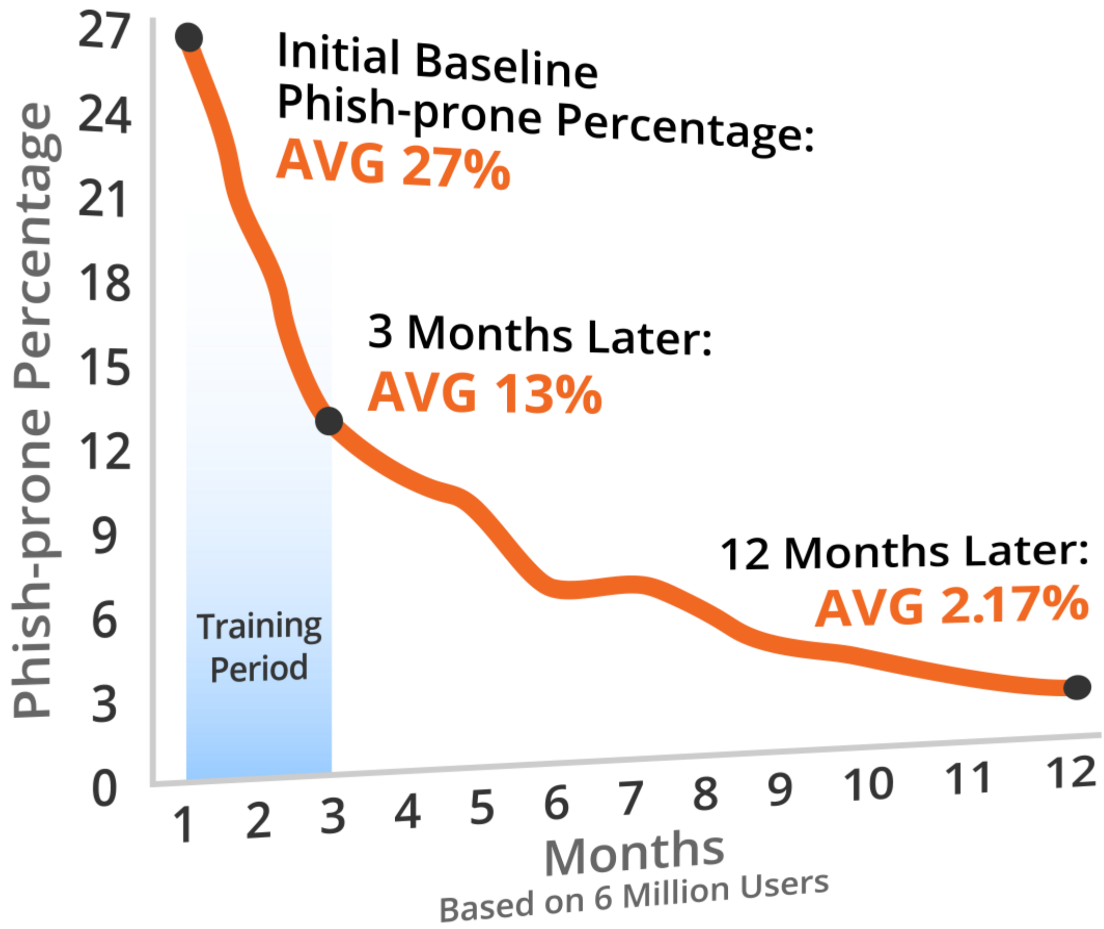
Phish Your Users
Fully automated simulated phishing attacks, hundreds of templates with unlimited usage, and community phishing templates.

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



Security Awareness Training Program That Works

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



Thank You!

Erich Kron – Security Awareness Advocate

ErichK@KnowBe4.com | @KB4Erich | @ErichKron

KnowBe4

Human error. Conquered.