Social Engineering and Business Email Compromise

What Do You Need to Know?

Presented by: Nick Podhradsky, EVP
and Buzz Hillestad, GCFE
SVP Consulting, DFIR Lead, CBFI Instructor

Contact Information

Follow us on Social:

- Nick Podhradsky
  - Executive Vice President Business Development Master's of Educational Technology, Dakota State University
  - Mission: Help business leaders make better cybersecurity decisions
  - Phone: 605-770-3926
  - Nick@sbscyber.com
  - www.sbscyber.com

Contact Information

Follow us on Social:

- Buzz Hillestad, GCFE
  - SVP IS Consultant, Incident Response Digital Forensics Lead
  - SANS MEs: Ethical Hacking, Digital Forensics, and Incident Response
  - Mission: Disrupt and Deceive Cybercrime – and I LOVE MY JOB!
  - Email: Buzz.Hillestad@sbscyber.com
  - Website: www.sbscyber.com
  - Blog: https://buzzsec.blogspot.com/

- SBS DFIR Department (Emergencies Only)
  - IR@sbscyber.com
  - **Office: +1 (855) SBS-DFIR**

The time is nigh.

Cybersecurity risks are ever increasing and are only going to become more voluminous. Business leaders adopting a proactive mindset for their organization are prepared and ready for the eventual threats that will impact them.

Reactive or Proactive?

Challenges

- Unplanned Events
- Unexpected Results
- Unbudgeted Costs
- **FEAR**

Reactive

- Sudden Need

Proactive

- Plans

Why Now?

- Revenue Growth
- Nimble – Technology Adoption
- Profitability
- Secure Future

Are We Even at Risk?

- “We don’t have anything of value; why would someone want to hack us?”
- “We’re too small of a company for a hacker to target.”
- “We’re in a small, rural area; no one knows who we are.”
- “IT will take care of it.”
- “We’ve got a firewall, so we’re protected.”
- “We trust our people not to fall for scams.”
- “We’ve got insurance; we’re covered.”

No business is immune to cybercrimes!

Who is a Cybersecurity Target?

- Hackers use automated tools to search the internet for internet protocol (IP) addresses that are “alive.”
- Automatically looking at what type of device is attached on the IP address.
- Trying to identify weaknesses in the security of the device.
- Hackers generally don’t know who you are, where you are, or what you have, until they can compromise the device.
- establish a baseline of internet connected devices and then are notified when a new IP address attaches to the internet.
- Everything that touches the internet has an IP address.

You Are of Value to a Hacker

- Customer information

  Social security numbers, bank account numbers, birthdates, addresses, and contact information

- Employee information

  Social security numbers, bank account numbers, birthdates, addresses, and contact information

- Sensitive corporate information

  Trade secrets, software licenses

- Online banking information

  Usernames and passwords

- Email accounts

  Which can be compromised and used to send more phishing email or initiate email fraud attacks

- Social media accounts

  Which can be compromised to spread false information or defamatory statements

- Computer assets

  Hackers can use to host their information, serve as pivot-points for other attacks, or use to attack (DDos) other computers or networks

Social Engineering

What Is It?

Social Engineering?

- Nontechnical way to get information
- People are predictable
- We all have certain “programming”, these programmed responses can be “gamed” to trick people into divulging information or even giving access to something.

Most Prevalent Threats

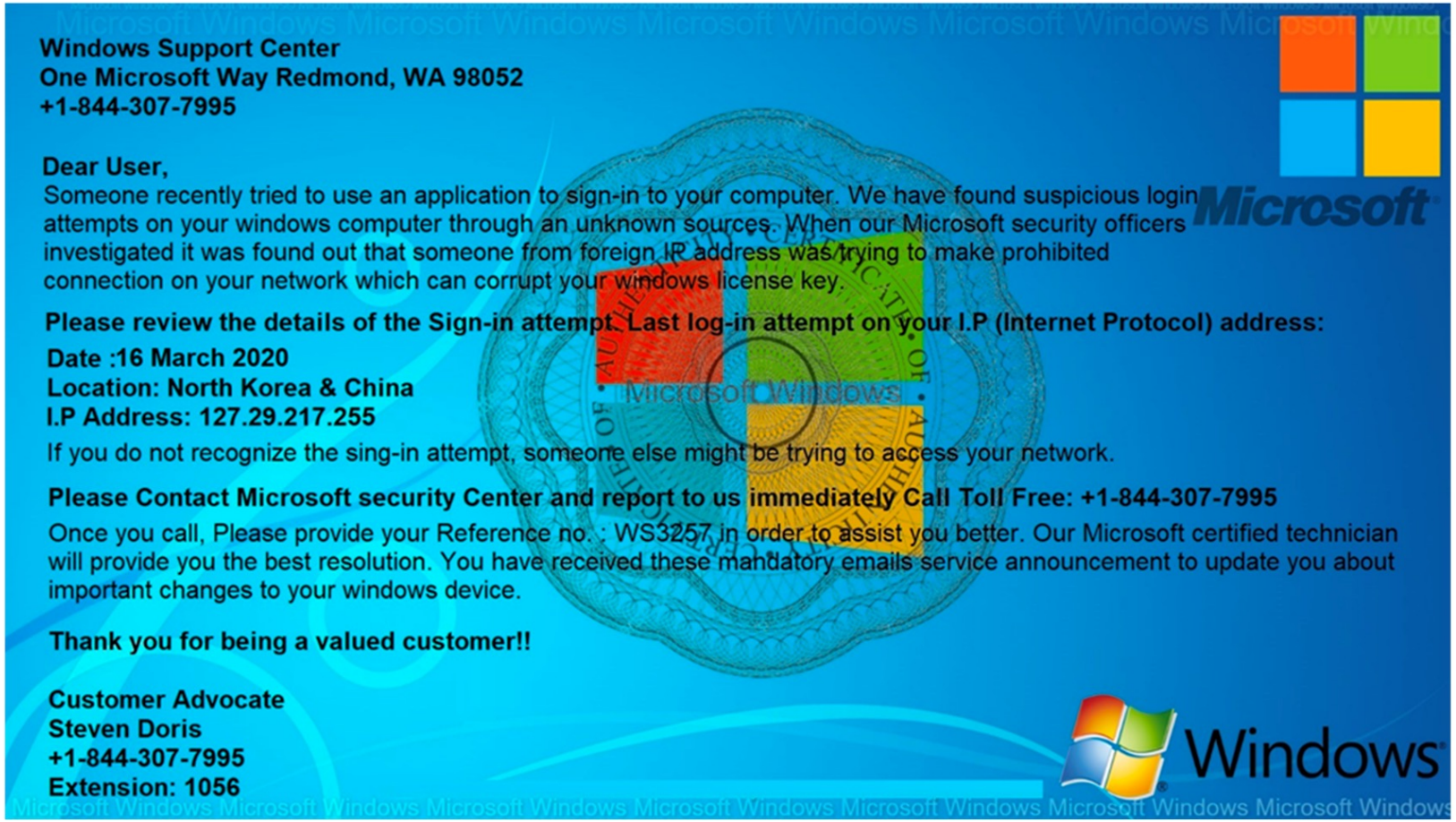
- Social Engineering
  - Phishing
  - Pre-text calling with spoofed numbers
- Business Email Compromise
  - What is it?
  - How does it happen?
  - How can you protect your organization?
  - Real world examples

Phishing

- The attacker generates an email that is very believable or tricky
- In some recent cases, the attacker has compromised an upstream email account of someone the victim has done business with before
- The attacker tricks the victim into giving up their username and password
- In other cases, the attacker tricks the victim into clicking a link or opening a file that will steal username and password or compromise the computer or the computer accounts

Phishing Example: Scare Tactics

From: Microsoft Securities <microsoftsecuriies@gmail.com>
Sent: Monday, March 16, 2020 5:09 AM
Subject: WINDOWS SECURITY ALERT !!



Phishing Example: Scare Tactics

From: Juan Tipula <jtipula@hidrostal.com.pe>
Sent: Monday, March 16, 2020 6:43:52 PM
Subject: Email Notification (Treat Urgent)

Attention:

Your E-mail account was recently signed in from an unknown location.
Please click here for verification to avoid closure of your E-mail account

To complete this verification, simply or click here

Sincerely,
Email Support

Phishing Example: COVID-19

"Distributed via the CDC Health Alert Network
January 31, 2020
CDCHAN-00426

Dear [redacted]

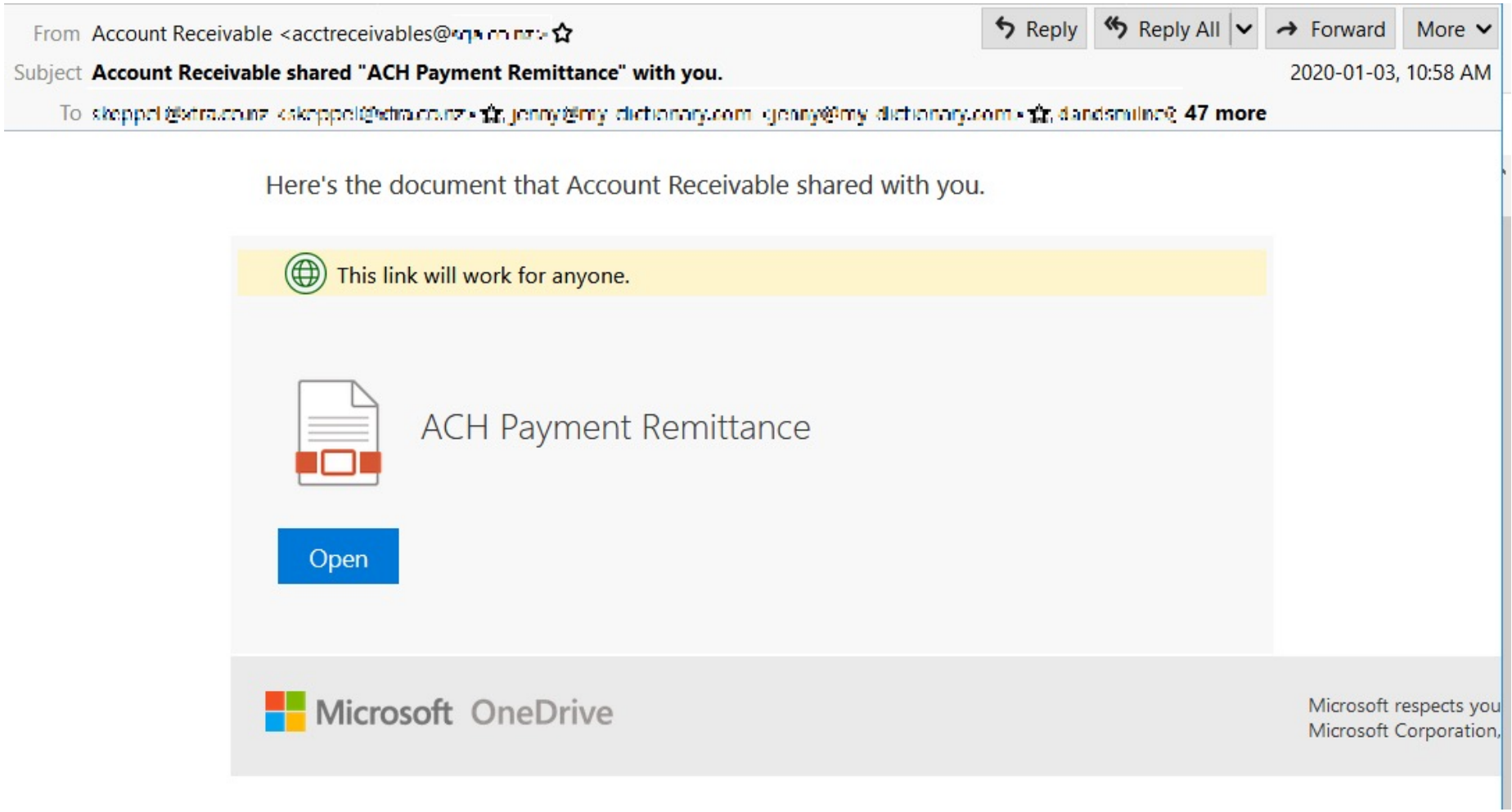
The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

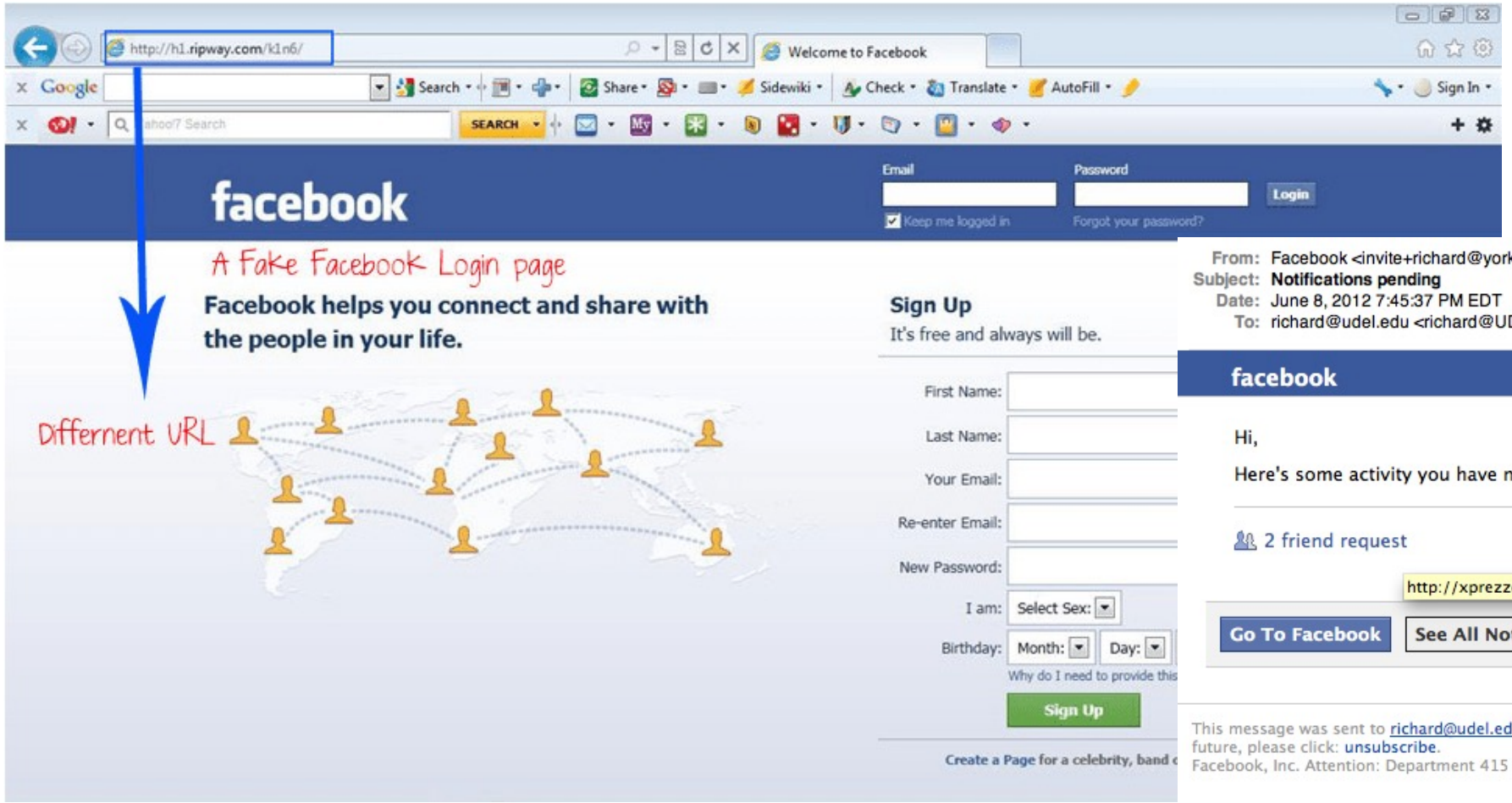
You are immediately advised to go through the cases above for safety hazard

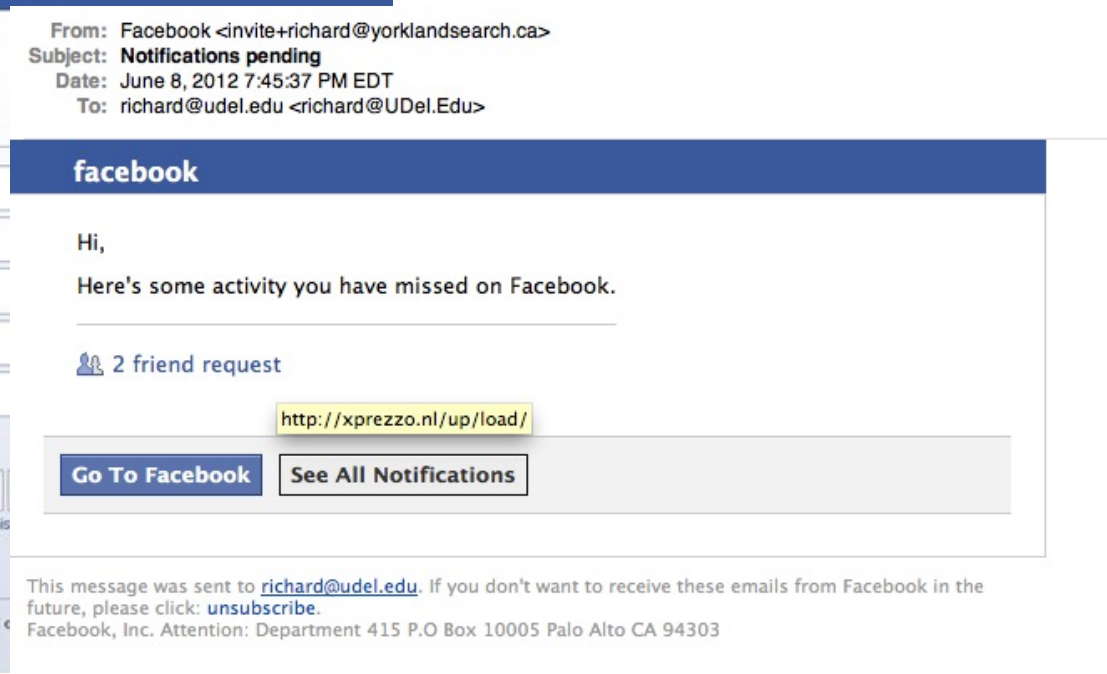
Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention"

Difficult to Identify?



Stealing credentials





Email

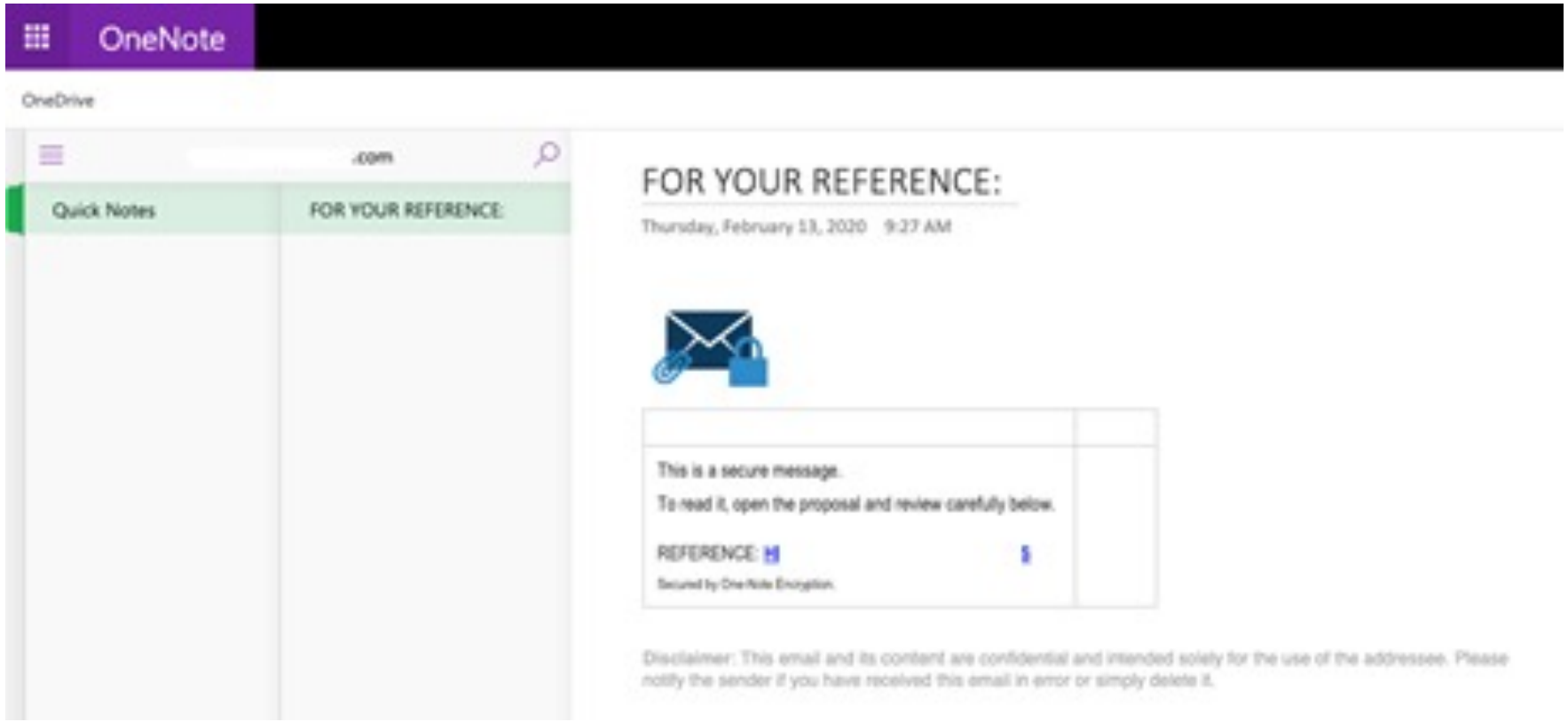
From: Jane Doe
Sent: Monday, August 31, 2020 10:45 AM
Subject: Title_Insurance_Agency_RFP_2020_08_31

A document has been shared with you by Jane Doe, the document was uploaded using pdf.

Click below to review the document attached. Title_Insurance_Agency_RFP_2020_08_31

Please let me know if you have any further questions.

Jane Doe | Escrow Agent
Title Insurance Agency


OneNote
OneDrive
.com
Quick Notes
FOR YOUR REFERENCE:
FOR YOUR REFERENCE:
Thursday, February 13, 2020 9:27 AM
This is a secure message.
To read it, open the proposal and review carefully below.
REFERENCE:
Secured by OneNote Encryption.
Disclaimer: This email and its content are confidential and intended solely for the use of the addressee. Please notify the sender if you have received this email in error or simply delete it.

From: support@drp-box.com

Reply-to: support@drp-box.com

Subject: Important File #45435 shared through DropBox

Send me a test email

Toggle red flags

Someone from your address book just shared an **IMPORTANT** document with you.

You can view or download your document below.

> **View Document**

> **Download Document**

Happy Dropboxing!

- The Dropbox Team

Pre-Text Calling

- Attacker spoofs a phone number and calls the victim
- Victim sees the phone number is that of who they claim to be and gives trust
- The attacker sometimes asks for information like account numbers or would like to change shipping addresses or some other type of attack
- In some cases, the attacker asks the used to visit a website (same as clicking on a phishing link) – example
- Sometimes the attacker has a lot of information to make the call very believable

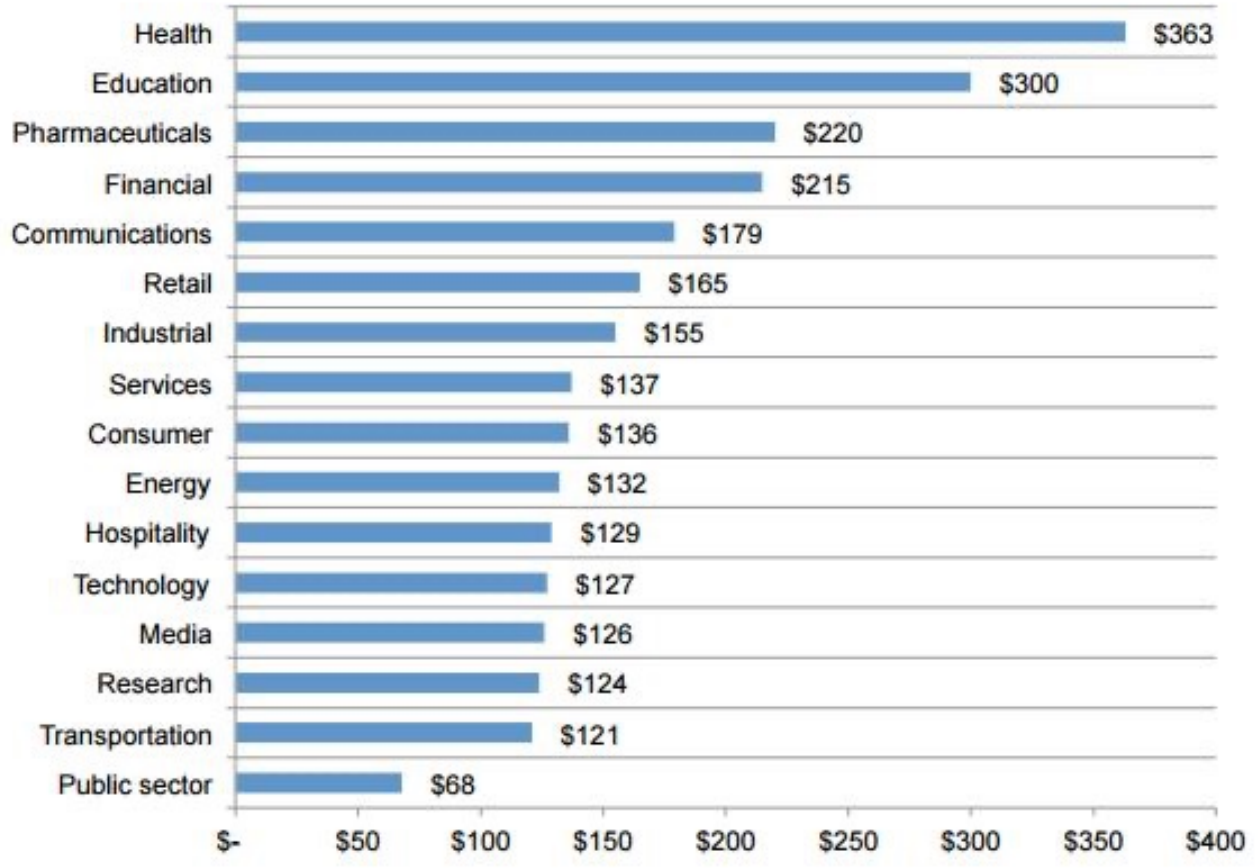
Business Email Compromise

What Is It and How Does It Work?

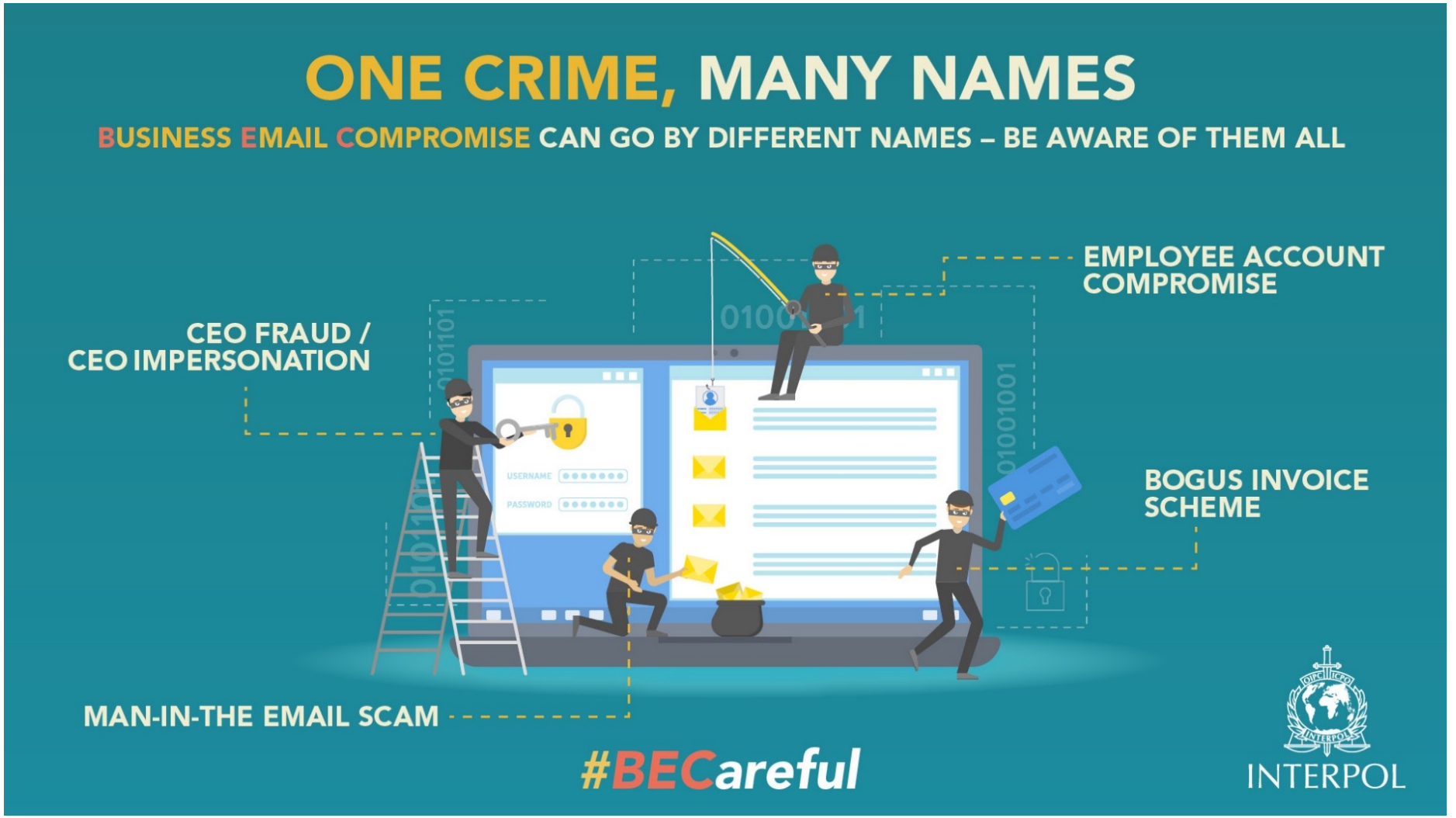
IC3

Business Email Compromise (BEC) is defined by the IC3 as “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 e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.”

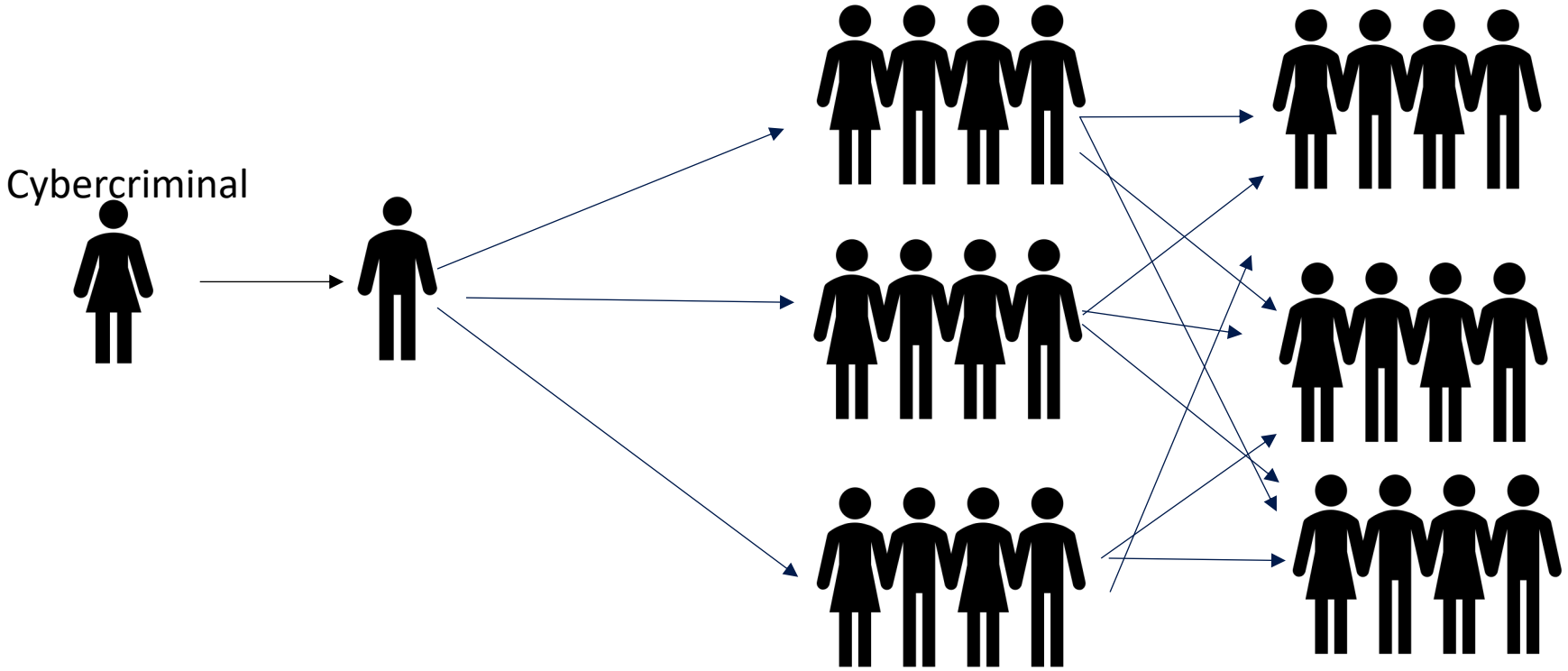
Figure 4. Per capita cost by industry classification
Consolidated view (n=350), measured in US$



Source Ponemon Institute

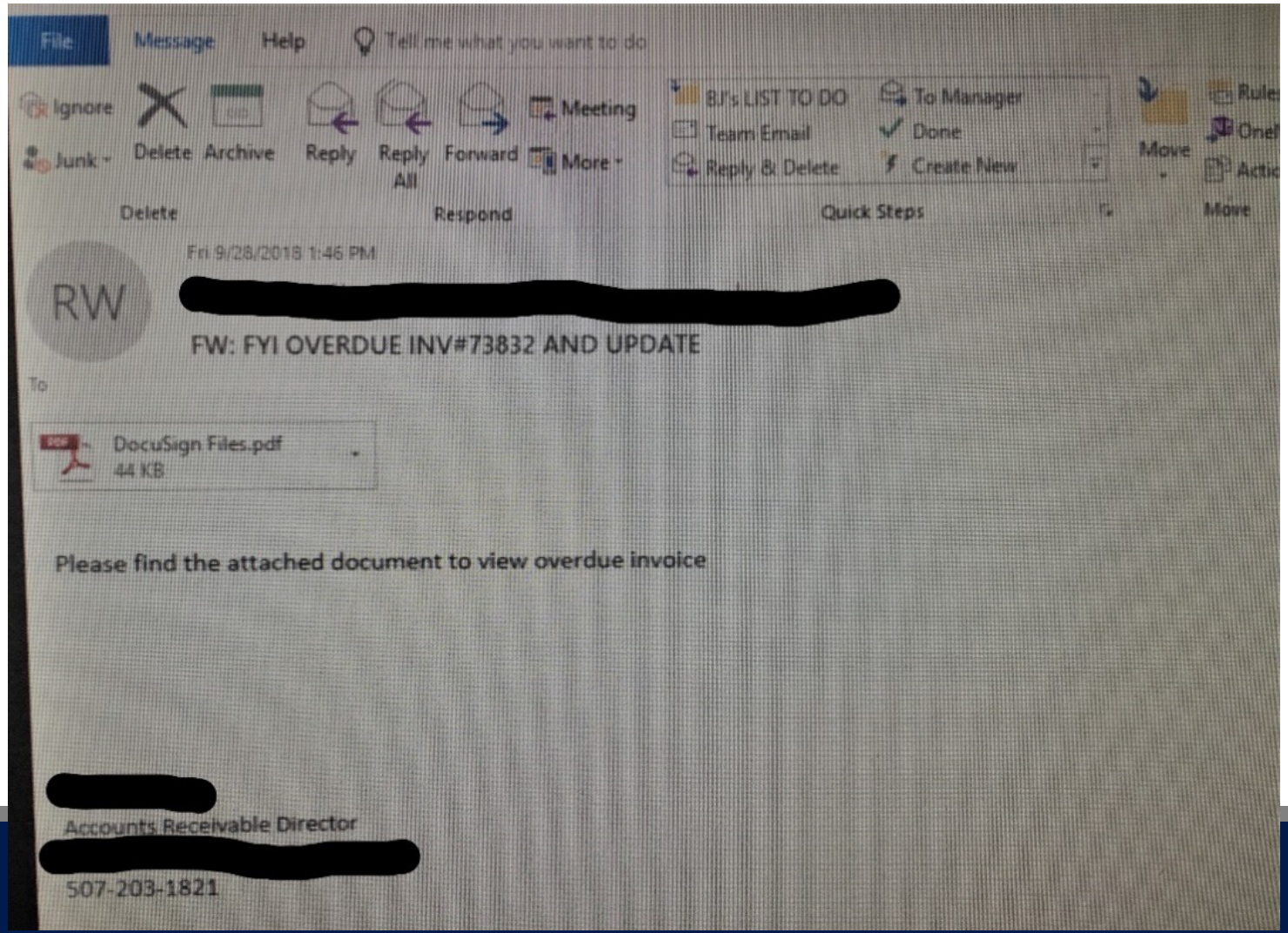

ONE CRIME, MANY NAMES
BUSINESS EMAIL COMPROMISE CAN GO BY DIFFERENT NAMES – BE AWARE OF THEM ALL
CEO FRAUD / CEO IMPERSONATION
EMPLOYEE ACCOUNT COMPROMISE
BOGUS INVOICE SCHEME
MAN-IN-THE EMAIL SCAM
USERNAME
PASSWORD
#BECareful
INTERPOL

How does it happen?



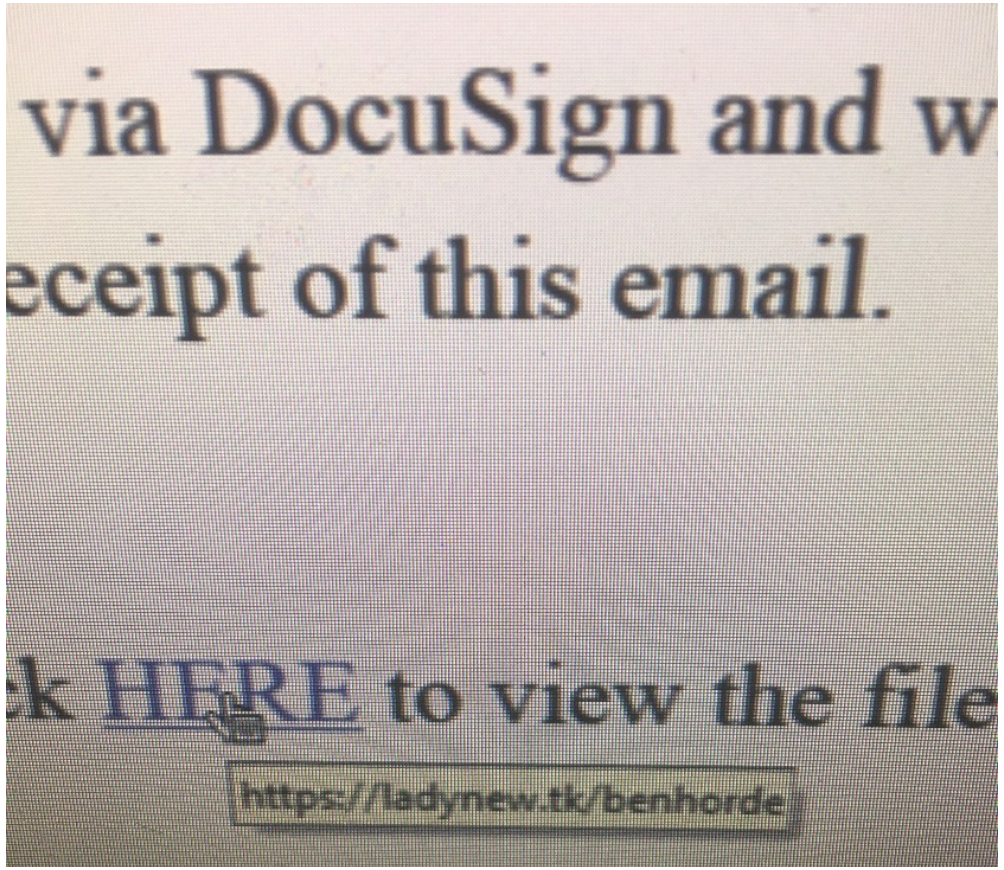
Email Account Takeover - Phishing

- The email used a PDF attachment that appeared to be from DocuSign, a well-known and highly utilized company for legally signing electronic files.



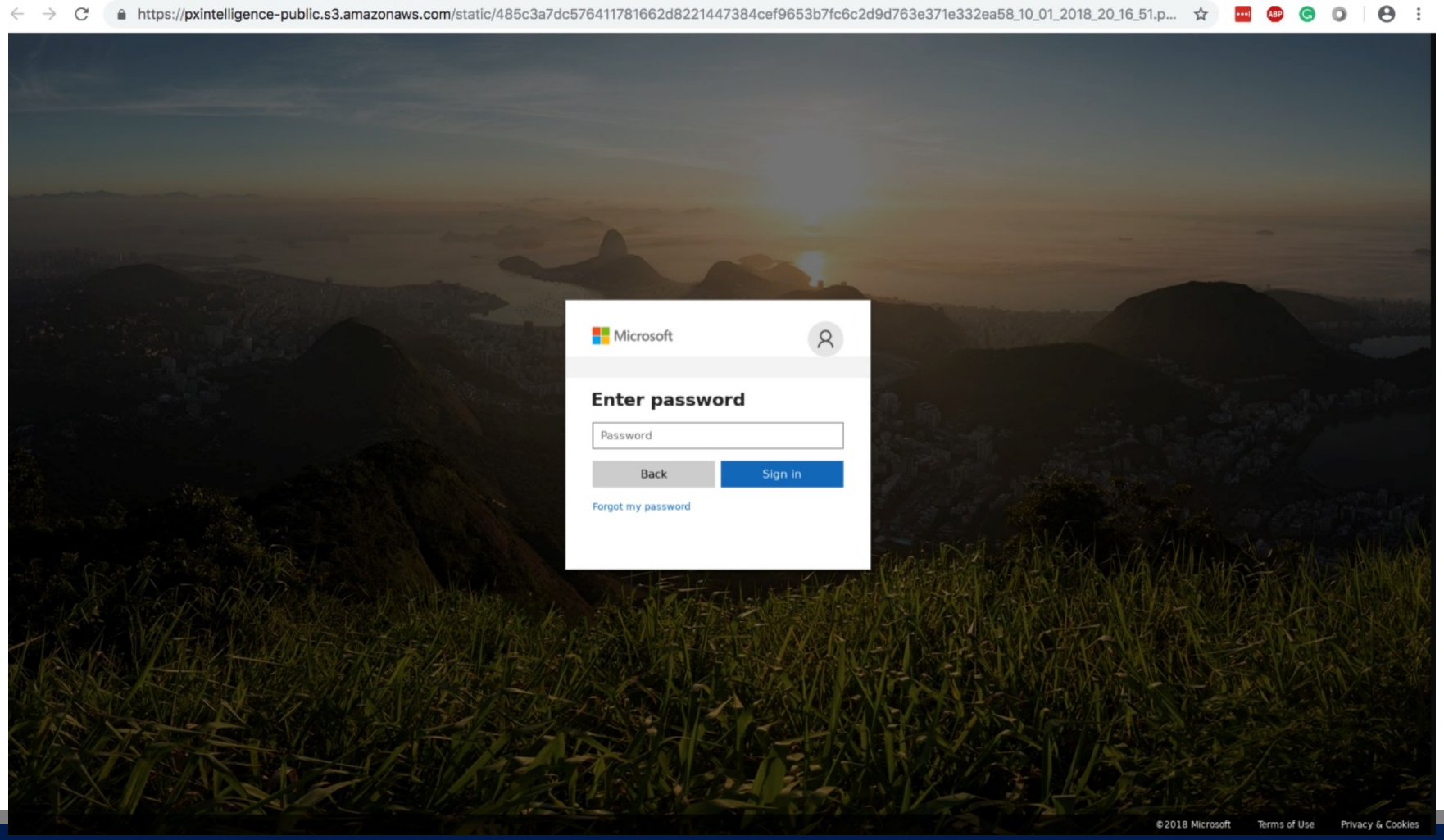
Email Account Takeover

Ultimately the only active content in it was a link as seen in the following image:



Email Account Takeover

- You can see their O365 portal was very convincing



Search Compromised Account

- Discover the flow of money and who the players are
- Search email history for key terms
  - Wire
  - Payment
  - Invoice

Create Rules or Attack

The attacker is working in your email while you are, so they hide their activities with these tactics.

Forward the inbox to another email address

Delete messages from upcoming target list

Email#1

Date: 3-14-2021
From: Accounts Payable (vendor@service.com) – this is very similar to the email address of your accounts payable person you're used to seeing 😈

To: Victim Pharma (you@yourcompany.com)

Subject: RE: Update To Payment Account

Good morning,

Please confirm when we can expect the next payment? There is an immediate update to our payment processing.

Thanks

Please let me know if you have any questions.

Accounts Payable

Jane Doe – they use someone you've done business with from searching your email

919-628-3567

Email#2

Date: 3-14-2021
From: Victim Pharma (you@yourcompany.com
To: Accounts Payable (vendor@service.com) 😈
Subject: RE: Update To Payment Account

Jane,

We will remit payment to the website as usual.

Thanks.

Pharma

Beth Hicks

Email#3

Date: 3-14-2021
From: Accounts Payable (vendor@service.com) 😈

To: Victim Pharma (you@yourcompany.com)

Subject: RE: Update To Payment Account

No, please do not make any payment on the website because our account information on the website for receiving payments has exceeded its tax- free limit. It's undergoing an audit and all incoming payments have been blocked on the account at the moment. Please confirm and I can forward you our updated ACH banking information to make the future payments direct from your bank account?

Accounts Payable

Jane Doe

919-628-3567

Email#4

Date: 3-14-2021
From: Victim Pharma (you@yourcompany.com
To: Accounts Payable (vendor@service.com) 😈
Subject: RE: Update To Payment Account

Jane,

Ok, please send the new ACH account information.

Pharma

Beth Hicks

Email#5

Date: 3-14-2021
From: Accounts Payable (vendor@service.com) 😈

To: Victim Pharma (you@yourcompany.com)

Subject: RE: Update To Payment Account

Our ACH routing number is 123456789

Our Account Number is 000123456789

Accounts Payable

Jane Doe

919-628-3567

Email#6

Date: 3-14-2021
From: Accounts Payable (vendor@service.com) 😈

To: Victim Pharma (you@yourcompany.com)

Subject: RE: Update To Payment Account

Please confirm if you got our updated billing information as we want our payment to go to our bank account via ACH Wire transfer. Kindly let me know when this will be paid so I can forward our detailed copy if not received.

Accounts Payable

Jane Doe

919-628-3567

Email#7

Date: 3-14-2021
From: Victim Pharma (you@yourcompany.com
To: Accounts Payable (vendor@service.com) 😈
Subject: RE: Update To Payment Account

Jane,

We have remitted payment as per your instructions. Please confirm you have received the payment.

Pharma

Beth Hicks

*Bad Actor has already arranged control of a named cryptocurrency wallet for the funds to be converted to

What Can Businesses Do?

- ACH Whitelisting
- Dual Authorization/Dual Signature
- In Person/Voice Verification or Call Backs – do not call the number in email
- Have tech firm enable logging/location access in email system
- Implement multi-factor authentication
- Enable Audit Logs in 0365
- Geo location IP Blocking
- Sandboxing
- Register domains that are similar to their business
- SPF, DKIM, and DMARC

SBS CyberSecurity

Who is it coming from?
What do they want?
Why do they want it?

Who is the Sender?
Do I know them?
Are there any misspellings?
Did I expect this email?

Why

- Why are they emailing me?
- Why are they asking me to take action.
- Is this even believable?
- Are they creating urgency?

Red Flags

- Unexplained urgency.
- Last minute changes in wire instructions or recipient account information.
- Last minute changes in established communication platforms or email account addresses.
- Communications only in email and **refusal to communicate via telephone** or online voice or video platforms.
- Different phone number from the one the person you're used to communicating with usually uses
- Requests for advanced payment of services when not previously required.
- Requests from employees to change direct deposit information.

Password Best Practices

- We are all consumers and we like convenience!
- 81% of hacking related breaches used either stolen or week passwords
- Do not use the same password on multiple systems.
- Passwords should be at least 10 characters (15, if possible) with 3 of the 4 characteristics of upper-case letter, lower case letter, number, or symbol.
- Avoid using a dictionary word in your passwords.
- Avoid using your personal elements such as username, first name, last name, phone number, family, towns, state, or Bank name in your passwords.
- Passwords should be replaced at least every 90 days and not reused for at least 12 months.

Password Managers

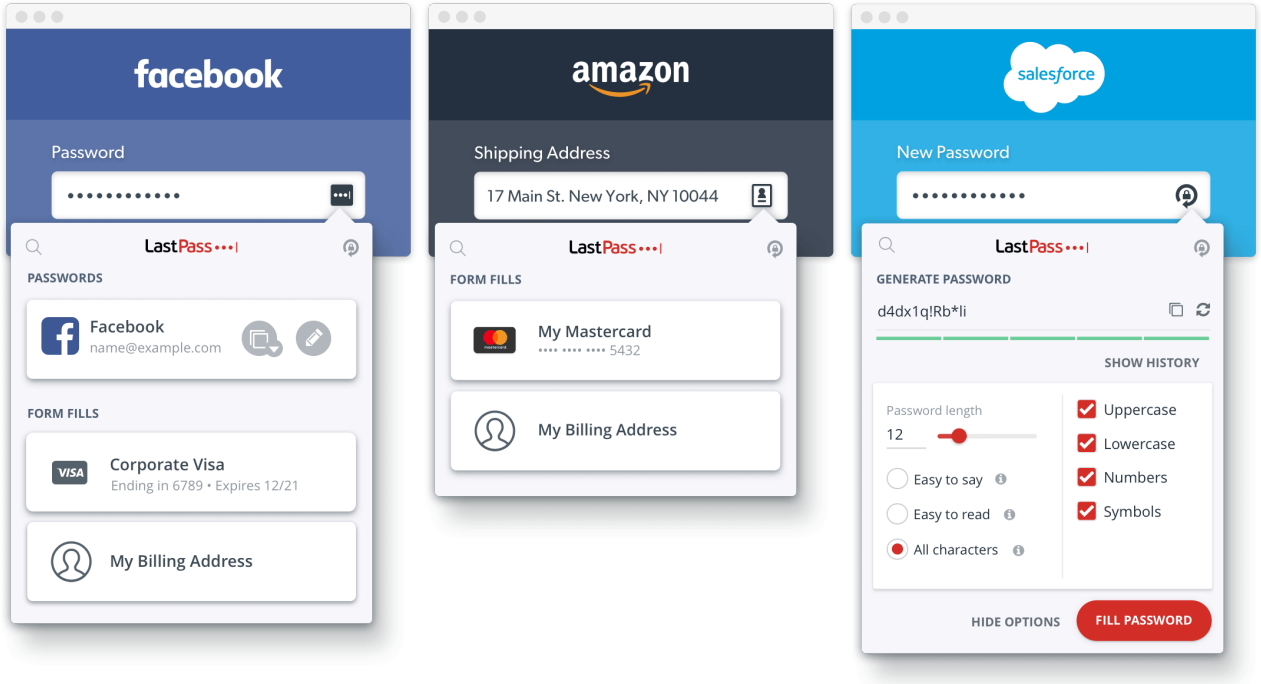
Category	Website /link	User Name	Account No./Name	PW
Banking	http://www.americanexpress.	FirstNameLastNa yahoo.com		bank123
Business	CRA		Business1	business123
Home	Town of Oakville	name@ya om		abc
Home	Enercare			home
Kids	https://login.schoolgatewa			1234
Personal	Yahoo			abc
Personal	Youtube		Name	abc123
Personal	CRA		123456789	1234
Personal	Facebook	FirstNameL ame		1234
Personal	Yahoo	FirstNameLast e@yahoo.com		12345
Personal	http://www.linkedin.com	FirstNameLastNa yahoo.com		1234
School	https://eportal.joshuacreekschool.ca		FirstNameLastName	school123
School	https://www.scopay.com	Name2@gmail.com		school124

Excel

KEEPER
Cybersecurity Starts Here™

KeePass

dashlane



SBS Resources

- https://www.sbscyber.com/education/free-downloads
- https://www.sbscyber.com/education/webinars
- https://www.sbscyber.com/education/blog

- https://sbscyber.com/resources/threat-advisory-business-email-compromise
- https://sbscyber.com/resources/threat-advisory-sim-swapping
- https://sbscyber.com/resources/threat-advisory-new-phishing-technique

Multi-Factor Authentication

Multi-Factor is a great way to reduce risk of unauthorized access. But like most things cybersecurity, it can be beaten.

Contact Information

Follow us on Social:

- Nick Podhradsky
  - Executive Vice President Business Development Master's of Educational Technology, Dakota State University
  - Mission: Help business leaders make better cybersecurity decisions
  - Phone: 605-770-3926
  - Nick@sbscyber.com
  - www.sbscyber.com