Monthly Cybersecurity Newsletter



Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer - Maria Thompson



The Billion Dollar Scam!

Business E-mail Compromise (BEC), also known as CEO fraud scams, is a sophisticated scam targeting both organizations and individuals that is on the rise. BEC comes in a variety of forms, such as deceiving employees into

sending money or personally identifiable information (PII), or using an organization's name to fraudulently obtain goods. The scam can involve compromising legitimate business e-mail accounts and requesting PII or Wage and Tax Statement (W-2) forms for employees. According to a recent Public Service Announcement (PSA) from the Federal Bureau of Investigation (FBI), there has been a 136% increase in identified global losses between December 2016 and May 2018 because of BEC scams. BEC scams have been reported in all 50 states and in 150 countries and have caused billions of dollars in damage. BEC is clearly a big problem.

Criminals use a variety of tactics to conduct BEC, from spoofing e-mail accounts and websites, to using spear-phishing attacks and malware. According to KnowBe4, a vendor that provides cybersecurity awareness and training content, 91% of successful data breaches start with a spear phishing attack. A BEC scam can start with a simple phishing email that may be hard to detect. These phishing emails have few of the tell-tale signs of traditional phishing messages, such as poor grammar and misspellings. But, like other social engineering attacks, urgency is a common tactic. Attackers play on the victim's fears and desire to help. Attackers may also spend weeks or months studying an organization's vendors, billing systems, and a CEO's style of e-mail communication and even travel schedules. Then, perhaps when the CEO is away from the office, the scammer sends a bogus e-mail that appears to be from the CEO requesting money to be sent. Targeted employees believe they are sending money to a familiar account, just as they have done in the past, but the account numbers are slightly different. If the money is sent, it will end up in a different account controlled by criminals.

What Can You Do?

- The best defense is to verify all financial transaction requests. Do not rely on e-mail alone. Confirm requests for fund transfers by using a secondary means of communication, such as phone verification using previously known numbers.
- Use multi-factor authentication (MFA), particularly for access to sensitive systems and data. MFA is more secure than a single factor (e.g. password alone) and helps mitigate the risks of credential theft.



- Be careful what personal information you share online, including job titles, promotions, and areas of influence in your organization. BEC actors use information that is publicly available on social networking sites, such LinkedIn, Facebook, and Twitter.
- Establish code phrases for phone conversations that are only known to legitimate parties. Victims have received phone calls from attackers requesting personal information for verification purposes – fraudulent phone conversations that were like legitimate ones.
- > Train staff in the finance or human resource departments to identify BEC scams.

If you discover a fraudulent transfer, it is important to respond to it quickly. Contact your financial institution and request a recall of the funds. Contact your local FBI office and report the fraudulent transfer. Finally, file a complaint with <u>www.ic3.gov</u>. The Internet Crime Complaint Center (IC3) can assist both the financial institutions and law enforcement in the recovery efforts.

Be sure to review the **Social Engineering Red Flags** flyer that is included at the end of this newsletter. It might be a good idea to print this out and have it handy as a quick reference.

How Safe Are Your Things?

"Internet of Things" (IoTs) devices include any electronic device that connects to the Internet. IoT devices can be anything from security cameras, routers, and refrigerators to printers, wearable devices, "smart" plugs and "smart" lightbulbs. IoTs add convenience to our lives, but they can also make us vulnerable to attack. Throughout 2016 and 2017, attacks from massive botnets, which are



networks of devices that are infected with malicious software and controlled as a group without the owners' knowledge, were comprised of hacked IoT devices. The FBI have warned that attackers are using IoTs as proxy servers to conduct their nefarious activities with anonymity. Some signs that an IoT is compromised include the following:

- A major spike in monthly Internet usage
- Devices become slow or inoperable
- Unusual outgoing Domain Name Service (DNS) queries and outgoing traffic
- Internet connections running slow

The following advice may reduce your chances of becoming a pawn to a cybercriminal:

- Connect only those devices you need
- Change default account names and passwords on all network devices
- Download and install the latest firmware updates and keep your devices updated
- Reboot devices regularly since most malware is stored in memory
- Place your IoT devices behind a firewall on your network
- Isolate IoTs from other network connections

- Avoid devices that advertise Peer-to-Peer (P2P) capabilities built-in
- Turn off IoT devices when they are not in use or not needed for a period of time ٠

Be sure to review this month's SANS Ouch! Newsletter on Smart Home Devices at the following link: https://www.sans.org/security-awareness-training/resources/smart-home-devices



The 14th Annual Triangle InfoSeCon will be held at the Raleigh Convention Center in Downtown Raleigh, North Carolina from 8:00 AM to 6:00 PM on October 26, 2018. For more information about this event, please visit http://www.triangleinfosecon.com/.



Newsletter various cybersecurity newsletters the distributes each month. We hope you find them beneficial. Don't forget the other **monthly newsletters** that are available to you. The following are the various cybersecurity newsletters the ESRMO

> SECURITYsense Newsletter: A licensed newsletter for State employees that contains several articles involving current cybersecurity issues. Note: You must have a Microsoft O365 account with access to the ESRMO external SharePoint site to access this resource.

https://ncconnect.sharepoint.com/sites/it ext/esrmo ext/Documents/Newsletters/SECURITYsense

Disclaimer: The SECURITYsense newsletter is a licensed product of the National Security Institute, Inc. (NSI) and is protected by the United States copyright laws. Distribution via an open Internet site (available to anyone with Internet access) or any other public access network is strictly prohibited.

Security Tips Newsletter: A free monthly cybersecurity newsletter from the Center for Internet Security (CIS). This month's edition is Want to keep your data? Back it up!

https://www.cisecurity.org/resources/newsletter

> SANS OUCH! Newsletter: A free monthly cybersecurity awareness newsletter provided by The SANS Institute. This month's edition is titled Smart Home Devices.

https://www.sans.org/security-awareness-training/ouch-newsletter



The SANS Institute also provides *free* awareness **videos** and **webcasts**. The SANS Video of the Month may be accessed via the following link: https://securingthehuman.sans.org/resources/votm.

The SANS Institute free webcasts may be accessed via the following link: https://www.sans.org/webcasts/upcoming.



National Preparedness Month (NPM) is in September. You can use the month to focus on your preparedness efforts for disasters and emergencies that affect where you live, work, and visit. The theme this year is "Disasters Happen. Prepare Now. Learn How." In addition to the theme for the month, the weekly themes highlight different preparedness actions. Help promote preparedness this September with NPM's web content and weekly themes:

- September 1-8: Make and Practice Your Plan
 - September 9-15: Learn Life Saving Skills
- September 15: National Day of Action
- September 16-22: Check Your Insurance Coverage
- September 23-29: Save For an Emergency

Visit <u>www.ready.gov/september</u> for all the NPM materials you can customize for your needs.



PCI Webinars by Coalfire

The following is a *tentative* schedule for webinars on PCI-DSS that will be presented in 2018. An announcement regarding each webinar will be sent about three (3) weeks prior to the scheduled date.

Date/Time: 10/9/2018 @ 10:00-11:00 AM ET Topic: Updates to the PCI DSS and PCI Hot Topics Presenter: Joseph D. Tinucci

Date/Time: 12/4/2018 @ 10:00-11:00 AM ET **Topic:** Managing Service Providers - Also address new Service Provider requirements in PCI

Other Upcoming Events...

August 29-30: Digital Government Summit, Hilton North Raleigh, Raleigh, NC

September 1: Agency Compliance Reports Due

September 1-30: National Preparedness Month

October 1-31: National Cyber Security Awareness Month

October 18-19: NC Cyber Awareness Stand-down

October 26: Triangle InfoSeCon





Do you have something to share? Is there a topic you would like to see in a future newsletter? The ESRMO encourages staff to share topics that will be of value to all agencies to foster better information sharing and awareness. If you have a suggestion for a topic that you would like for us to consider for a future newsletter, please send it to security@its.nc.gov.

Social Engineering Red Flags

FROM

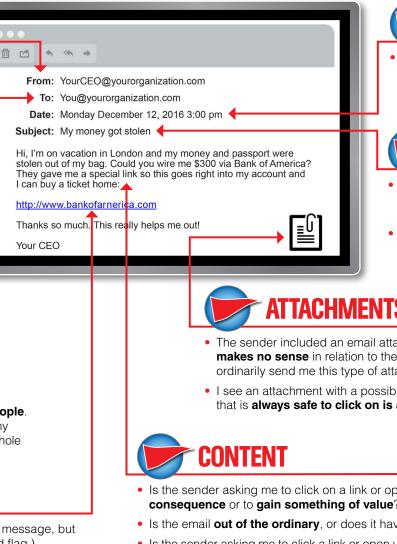
- I don't recognize the sender's email address as someone I ordinarily communicate with.
- This email is from someone outside my organization and it's not related to my job responsibilities.
- This email was sent from someone inside the organization or from a customer, vendor, or partner and is very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



- 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.



- 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."



DATF

Did I receive an email that I normally would get during regular business hours, but it was sent at an unusual time like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is irrelevant or does not match the message content?
- Is the email message a reply to something I never sent or requested?

ATTACHMENTS

- The sender included an email attachment that I was not expecting or that makes no sense in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is always safe to click on is a .txt file.
- 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?

