APRIL 26, 2022 // TUESDAY // ISSUE 6

SECURITY NEWS

BUSINESS EMAIL COMPROMISE

Seasons Change As Well As Attackers, So Do We

CHRIS MCDANIEL
APRIL 2022

Summer is almost here; the temperature is heating up and so are the attackers. As the season starts to change so do the attacker's methods. Attackers are always coming up with new ways to steal our information and do as much damage to us as they possibly can. So, we have to stay ahead of them so they don't defeat us. The Yadkin County Information Technology Department has introduced a new Security Awareness Training Platform. We have been working hard to come up with ways to better protect our employees as well as protecting the county. This training platform will provide everyone with the knowledge they need to protect their selves not only at work but also at home. Each month employee's will be introduced to a new security topic like Common Threats, Security Awareness Essentials, Social Engineering, and so many more. Please take time to complete these trainings and learn some great new tips and tools that will help you everywhere.

Please take time to read over this month's newsletter and also complete your monthly training. Remember the attackers are out there constantly looking for new ways to steal our information. Let's not fall prey to their tricks and work hard to keep them away. Remember to think before you click. Hope Everyone has a Great Day and Stays Safe.

Virtual Meeting Platforms and Business Email Compromise Scams

NCDIT
APRIL 1, 2022

The FBI Internet Crime Complaint Center has observed over the last three years a rise in business email compromise scams involving the use of virtual meeting platforms, according to a February public service announcement.

Criminals began using them in multiple ways due to the rise in remote work because of the COVID-19 pandemic, which caused more workplaces and individuals to conduct routine business virtually.

In one scenario, the FBI says, a bad actor compromises the email of an employer or financial director (such as a CEO or CFO) and requests employees participate in a virtual meeting platform. The criminal inserts a photo of the email sender with no audio, or "deep fake1" audio, and claims the video or audio is not properly working. The criminal then instructs employees to initiate transfers of funds via the chat or in a follow-up email.

Other techniques bad actors are using, the FBI says, include:

- Compromising employee emails to insert themselves in workplace meetings via virtual meeting platforms to collect information on a business's day-to-day operations.
- Compromising an employer's email, such as the CEO, and sending spoofed emails to employees instructing them to initiate transfers of funds, as the CEO claims to be occupied in a virtual meeting and unable to initiate a transfer of funds via their own computer.

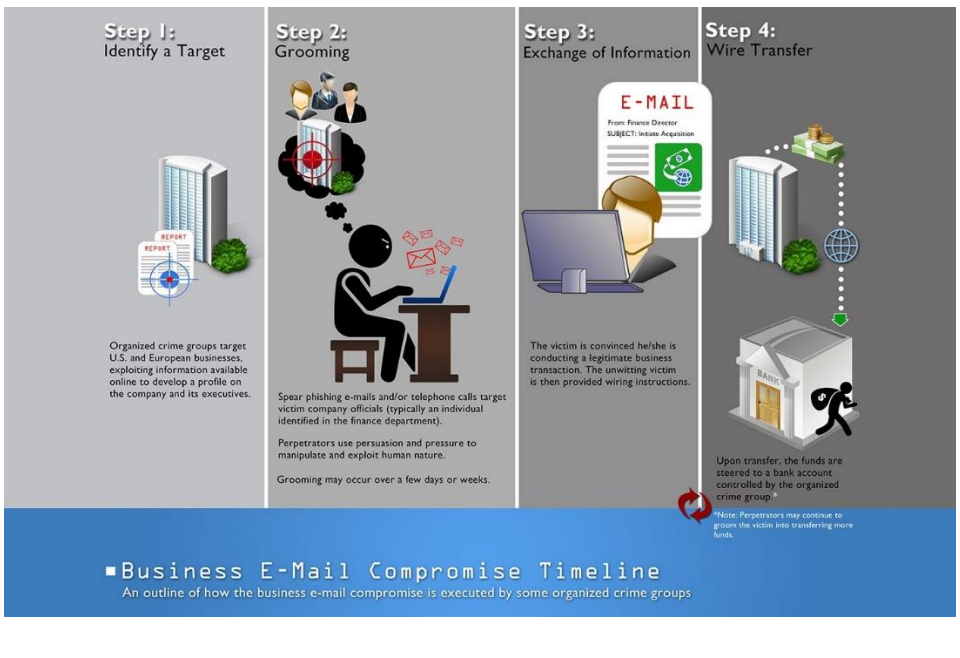
The FBI offers the following recommendations to help people avoid falling for these attacks:

- Confirm the use of outside virtual meeting platforms not normally used in your internal office setting.
- Use secondary channels or two-factor authentication to verify requests for changes in account information.
- Ensure the URL in emails is associated with the business/individual it claims to be from.
- Be alert to hyperlinks that contain misspellings of the actual domain name.
- Refrain from supplying login credentials or personally identifiable information of any sort via email. Be aware that many emails requesting your personal information might appear to be legitimate.
- Verify the email address used to send emails, especially when using a mobile or handheld device, by ensuring the sender's address appears to match who it is coming from.
- Monitor your personal financial accounts on a regular basis for irregularities, such as missing deposits.

This article provided by the NCDIT may be found via the link provided here: NCDIT.

Business Email Compromise

FBI, April 2022



What is Business Email Compromise?

Business email compromise (BEC) – also known as email account compromise (EAC) is one of the most financially damaging online crimes. It exploits the fact that so many of us rely on email to conduct our daily business but personally and professionally.

In a BEC scam, criminals send an email message that appears to come from a known source making a legitimate request, like these examples:

- A vendor your company regularly deals with sends over an invoice with an updated mailing address.
- A company CEO asks her assistant to purchase dozens of gift cards to send out as employee rewards. She asks for the serial numbers so she can email them out right away.
- A homebuyer receives a message from his title company with instructions on how to wire his down payment.

Versions of these scenarios happened to real victims. All these messages were fake. In each case, thousands – or even hundreds of thousands – of dollars were sent to criminals instead.

How Criminals Carry Out BEC Scams

A scammer might:

- **Spoof an email account or website.** Slight variations on legitimate addresses (john.kelly@examplecompany.com vs. john.kelley@examplecompany.com) fool victims into thinking fake accounts are authentic.
- **Send spearphishing emails.** These messages look like they're from a trusted sender to trick victims into revealing confidential information. That information lets criminals access company accounts, calendars, and data that gives them the details they need to carry out the BEC schemes.
- **Use malware.** Malicious software can infiltrate company networks and gain access to legitimate email threads about billing and invoices. That information is used to time requests or send messages so accountants or financial officers don't question payment requests. Malware also allows criminals to gain undetected access to a victim's data, including passwords and financial account information.

How to Protect Yourself

- Be careful with what information you share online or on social media. By openly sharing things like pet names, schools you attended, links to family members, and your birthday, you can give a scammer all the information they need to guess your password or answer your security questions.
- Don't click on anything in an unsolicited email or text message asking you to update or verify account information. Look up the company's number on your own (don't use the one a potential scammer has provided), and call the company to ask if the request is legit.
- Carefully examine the email address, URL, and spelling used in any correspondence. Scammers use slight variations to trick your eyes and gain your trust.
- Be careful what you download. Never open an email attachment from someone you don't know, and be wary of email attachments forwarded to you.
- Set up two-factor (or multi-factor) authentication on any account that allows it, and never disable it.
- Verify payment and purchase requests in person if possible or by calling the person to make sure it is legitimate. You should always verify any change in account number or payment procedures with the person making the request.
- Be especially wary if the requestor is pressing you to act quickly.

How to Report

If you or your company fall victim to a BEC scam, it's important to act quickly:

- Contact your financial institution immediately and request that they contact the financial institution where the transfer was sent.
- Next, contact your local FBI field office to report the crime.
- Also file a complaint with the FBI's Internet Crime Complaint Center (IC3).

The information for this article was provided by the FBI and may be found via the link provided here: FBI Scams and Safety.

Kevin Mitnick Security Awareness Training

Don't Become a Victim!

Cybercrime is big business—and happens more often than you think! Be aware of the tactics and attacks hackers use on YOU.

Kevin Mitnick, "The World's Most Famous Hacker" and KnowBe4's Chief Hacking Officer, will provide you with information about cyberthreats, as well as the key takeaways that can help minimize the risks you and your organization face.

TACTICS

Information Gathering

Social media is a gold mine of information hackers can use to trick you and your co-workers. Each piece of additional information gathered increases their odds for a successful attack. Some examples of things you should never share are travel plans, your organization's internal processes, or less obvious pieces of information like reports, financial information, or even the software your organization uses.

Takeaways: Be careful what you share. Ask yourself if the information you're about to post will be useful in conning you or your co-workers. Make sure you're familiar with your organization's expectations regarding what and how much you can share on social media by following your organization's social media policy.

Fake Profiles

Hackers use the information readily available through social media and online search engines to create an online persona that gets your attention. Their goal is to gain your trust and get you to take an action, like opening an attachment, clicking on a link, sending money, or giving them information to make their next attack more successful.

Takeaways: Never assume the security settings on social media sites will keep you safe from a fake profile attack. Be wary anytime you are asked to take an action on any site.

Disinformation

This is where hackers create and distribute false information to manipulate your thoughts and actions and cause damage to you or your organization. This strategy has become more common because of how fast information travels across social media networks.

Takeaways: Anything that tugs at your emotions is a warning sign. Always fight the spread of disinformation by verifying information's truthfulness. Stop and fact-check before acting upon or sharing information.

ATTACKS

Physical

Hackers might try to steal information using physical access. They might "tailgate" you or one of your co-workers, which is when they will act like they work there and follow you into the office. They might also use a uniform or stolen key card to get access to unlocked workstations or valuable information left out on desks.

Takeaways: Stay aware of your surroundings. Don't let anyone you don't know in. Always lock your devices when they're not in use, even if you're stepping away for a moment. Also, adopt a clean desk policy, which means keeping important items locked away when not in use.

Phishing

This is the method most often used by hackers. They use emails disguised as contacts or organizations you trust so that you react without thinking first. Their goal is to trick you into giving out sensitive information (i.e., your username and password), or taking a potentially dangerous action (i.e. clicking on a link or downloading/opening an infected attachment).

Takeaways: Phishing attacks are the most common type of attack because of how effective they are. Hackers are really creative when they target you, and it can be very difficult to tell if a message is real or fake. Stop, look, and think before you click that link, open that attachment, or share sensitive information.

Pretexting

Hackers sometimes use a made-up scenario to gain your trust so they can get the information they want. For example, they'll call and pretend to be on your IT team, mentioning the names of individuals they found while researching your organization. Then, they will say some updates just rolled out, and they need to validate a few things on your workstation.

Takeaways: Since this attack is convincing and prevalent, be vigilant. Never give information over the phone, in person, or online unless you've confirmed the identity of the person asking. You can do this by calling the person back using a verified phone number, on the organization's phone directory or main website.

Wireless Connections

More and more organizations are allowing their employees to work in places away from the actual office. Coffee shops, libraries, and even public parks often offer Wi-Fi connections that can be conveniently used to connect to the office as well as the internet. Be cautious as these Wi-Fi connections can be unsecure, and hackers want to see what you are doing online.

Takeaways: Never connect to public Wi-Fi unless you are using an organization approved VPN or Virtual Private Network. This technology creates a safe internet connection that shields your online activity from criminals.


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.
From: hr@yourorganization.cnet
To: judy@yourorganization.net
Date: Tuesday, December 3:00 AM
Subject: Survey
Hi Judy,
Now that our new CFO has been selected and starting soon, I'm asking everyone to fill out this quick survey so all the accounting functions can be captured. It should take you only few minutes. Must be completed by the end of the day.
Click here to take the [Survey] or download the attachment.
Thanks in advance for your cooperation!
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.
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 website. 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?
© 2016-19 KnowBe4, LLC. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.
KnowBe4
Human error. Conquered.