Email Compromise

Don’t be a Victim

Disclaimer

The information contained herein has been prepared for general informational purposes only and is not offered as and does not constitute legal advice or legal opinions. You should not act or rely on any information contained herein without first seeking the advice of your legal counsel.

No copy or use of this presentation should occur without the permission of Vizo Financial. Vizo Financial retains all intellectual property interests associated with this presentation. Vizo Financial makes no claim, promise, or guarantee of any kind about the accuracy, completeness, or adequacy of the content of the presentation and expressly disclaims liability for errors and omissions in such content.

"Email Compromise Attacks – Don't be a Victim" discussed in this presentation is the current version with effective date of 12/15/2021.

The comments today are my own and not necessarily those of Vizo Financial or the Vizo Financial membership.

Who Am I

Information Security Analyst for Vizo Financial

With the Corporate for 8 years

Working in Information Technology and Information Security

Career

24 years in the Banking and Investment Industry

19 of those years spent in Information Technology and Info Sec

Agenda

- Threat
- Email Account Takeover
- Business Email Compromise
- Defenses
- Questions

Threat

Bad Start to the Day

- Cannot log into your Core
- “Forgot My Password”
- Cannot log into your email
- Several $25,000 Wires

Please Leave it Active

- **Staff Member leave the company**
- **Email account not disabled**
- **Staff start to get odd email from former employees**

What Happened?

Email Account Takeover

What is Email Account Takeover?

- It is an exploit in which the bad-actor gains access to your legitimate email account credentials.
  - Personal email
  - Business email

- Often used as a starting point to other types of attacks.

Email Account Takeover

- Phishing email leading to a fake login page
- Brute Force password guessing
- Credential Stuffing
- Malware - Keylogger
- Known Password - from another data breach
- Poor Password Habits
- Social Engineering / Social Media

Threat

Email from CEO?

From: Bob_Bossman@acmecorp.com

To: Steve@acmecorp.com

Subject: FYI

I've just had some news from our attorneys confirming that we are in the final stages of completing a very important acquisition for the company. Having been privately negotiating this acquisition for a number of months it's great news we are finally so close to closing.

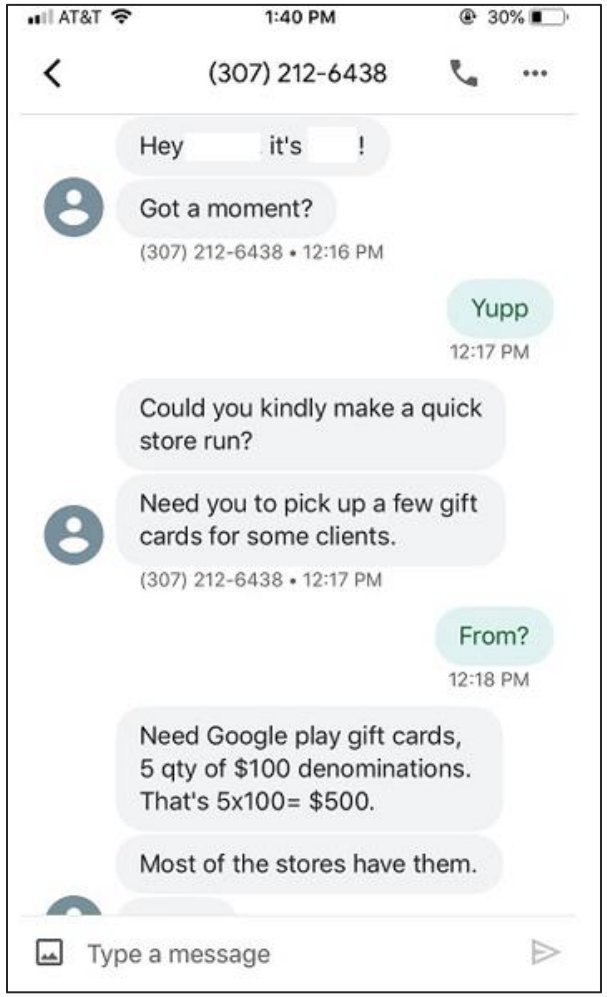
I will need you to make a wire payment today in the form of a deposit for the acquisition. Use this email as my full approval for this and any additional wires that may be required in the coming days.

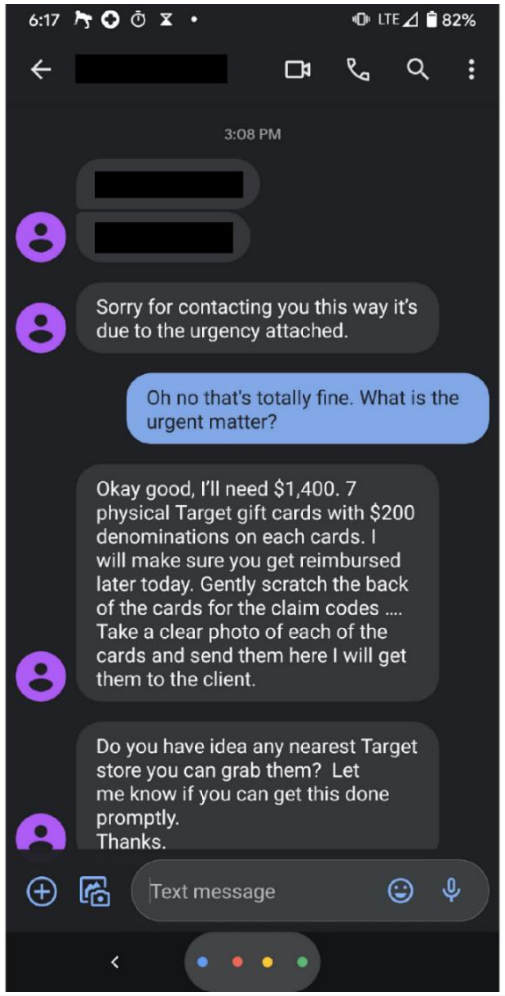
It's been agreed that, at this stage, the acquisition needs to remain private, so I have arranged for the lead attorney, John Jones, to contact you directly. He will work with you to ensure we have everything completed in line with the terms agreed.

If you have any questions, please relay them directly to John as he will be updating me on progress.

Regards

Text Message from CEO?





Business Email Compromise

What is Business Email Compromise?

- It is an exploit in which the bad-actor imitates the identity of someone in a position of authority or trust within an origination in order to obtain money or data.
  - Most commonly in email
  - Both external and internal

- Relies on the pre-established trust built between the victim and the assumed identity.

What is Business Email Compromise?

- It is a type of Social Engineering attack called Spear Phishing

- An attempt to acquire money or sensitive information by a method not easily undone.
    - Wire Transfers
        - Domestic
        - International
    - Gift Cards
        - iTunes / Google Play
        - Target / Walmart / Amazon
    - HR Data
        - Tax Information (W2)

Business Email Compromise

- 12% of “spear phishing” email are Business Email Compromise (BEC)*
- 13% of “spear phishing” attacks come from internally compromised accounts*
- 71% of “spear phishing” attacks include malicious URLs…*
  - Only 30% of BEC attacks include malicious URLs*

*March 2021 article from Barracuda Networks

Business Email Compromise

How business email compromise works

Defenses

Defense - Better User Access Controls

- Principle of Least Privilege
- Stop Sharing Accounts
- Better “off-boarding” procedures
- Security Awareness Training (NCUA 748 Part A)
  - NCUA recommends annual training

Defense – Share What You Know

- **Share the Information you have with others:**
  - Nigerian Prince Email
  - Do you share everyday examples you see?
  - Part of the Bad Actors' success is based on **our** lack of knowledge

Defense – Email Configuration

- Better Email Configuration
  - DNS-SPF Configured
  - Spam Filtering
  - Spoof Intelligence
  - External Email Alert
  - SSL Preferred
  - Secure Email Option
  - Have Your Own Email Domain

Defense - Better Passphrase Habits

- Passphrase - Protection with Mandatory Parameters
  - Enforced by the system – not manual
  - Use complex passphrases
    - Do not use dictionary-based passwords
  - Unique to each system
    - Passphrase Manager
  - Change or disable default system accounts

Defense – MFA / 2FA

- 2FA vs MFA – Choose wisely
  - Something you ARE / KNOW / HAVE
  - 2FA superior to MFA
  - Weaker
    - Security Questions
    - Email
  - Stronger
    - Physical Token
    - Software Token

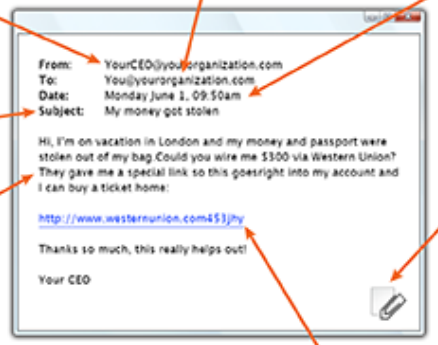
Social Engineering Red Flags

KnowBe4
Human error. Conquered.

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 hadn't communicated with recently.

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, a seemingly random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

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?**

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 these types of attachment(s).)
- 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.

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?

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" & "n".

Don’t Be Dave……

Questions