Seeing Through the Kaleidoscope of Risk

Ransomware & Email Compromise

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.

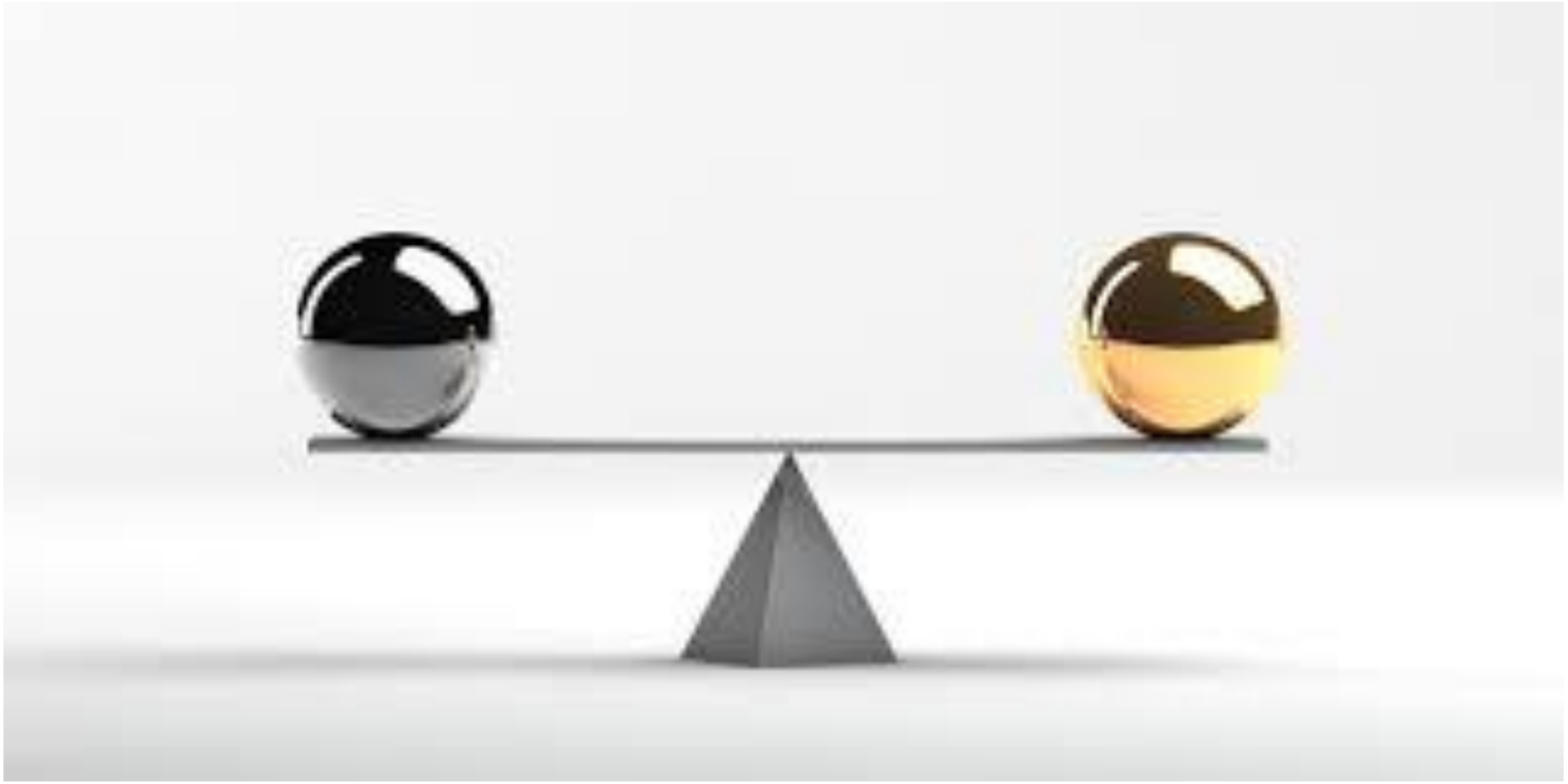
"Security Threats: Seeing Through the Kaleidoscope of Risk" discussed in this presentation is the current version with effective date of 3/28/2023.

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

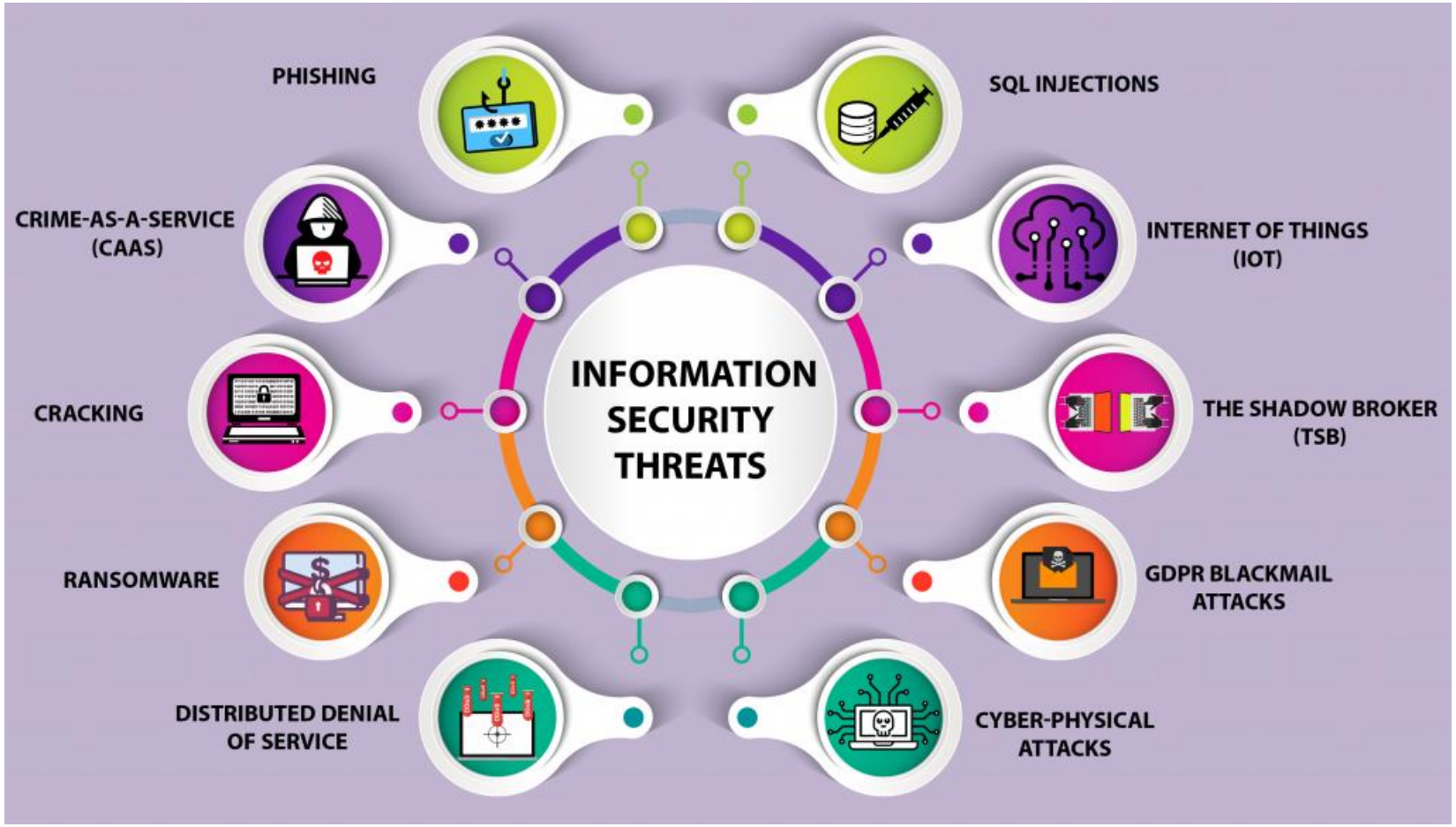
Agenda

- Balance
- Ransomware
- Email Account Takeover
- Business Email Compromise
- Questions

Finding Balance



Kaleidoscope of Risk



Ransomware

What is Ransomware?

- It is an exploit in which the bad-actor gains access to your network through a vulnerability / security weakness / or social engineering. Once in your network they lock your access to data, encrypt your data, or otherwise restrict your access to it until a ransom payment is made.

Ransomware Costs

- Coalition’s 2022 Cyber Claims Report mid-year update
  - Small businesses are a more attractive targets
  - 2021 to 2022 average claim cost has increased 58% to $139,000

  - Number of Ransomware attacks has decreased from last year
  - Ransom dollar amounts has also decreased from $1.37 million to just under $900,000

Ransomware History

- 1989 - AIDS Trojan
  - Harvard educated biologist mailed 20,000 floppy disks to WHO
  - Questionnaire about the HIV epidemic (social engineering)
  - Simple encryptor to block users for accessing files
  - Mail $189 to a PO Box in Panama for decryption key

Ransomware History

- 2004 - Use of Phishing email becoming common
  - Use of custom encryption algorithm
  - Only asked for $20 to unlock system
- 2006 – First use of 1024-bit RAS encryption codes
  - All victims all has the same description key
- 2012 - Fist RaaS available to lower skilled hackers
  - Fist demand to pay in crypto

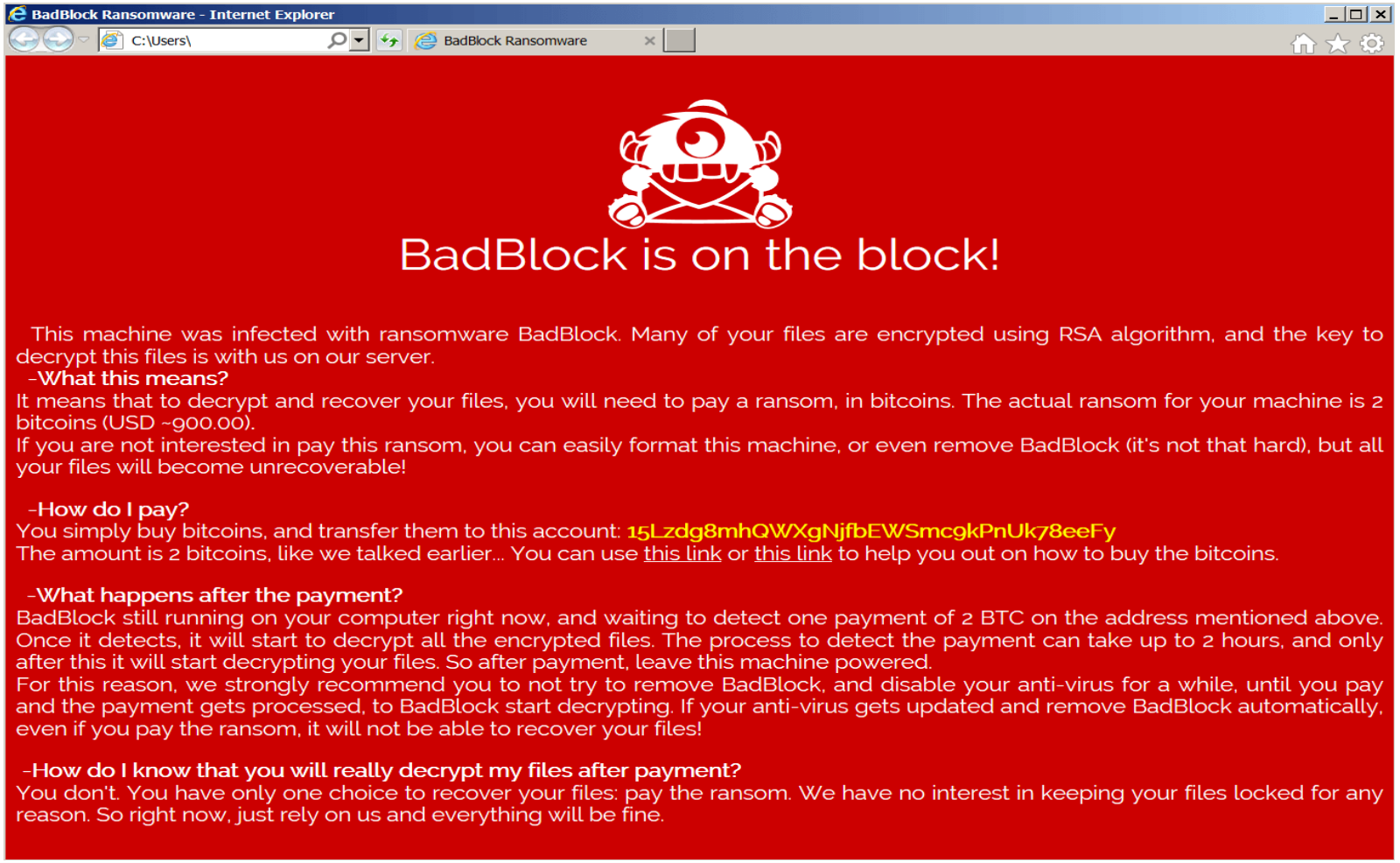
Ransomware History

- 2013 - First use of 2048-bit RSA encryption codes
  - First ransomware that was both a locker and encryption
  - Propagated as an email attachment

- 2016 - First encrypt of the master file table
  - Not just individual file encryption, but whole hard drive

- 2017 – WannaCry hits 150 plus countries
  - Financial Institutions / Healthcare / Law Enforcement / Education

Ransomware Types



Ransomware Types

- Crypto Ransomware (encryptors)
  - Most common / most damaging
  - File and data are encrypted and made unusable

- Locker Ransomware
  - Locks the operating system
  - File are not usable because they are not accessible

Ransomware Types

- Doxware (leakware)
  - Making company trade secrets public
  - Posting of sensitive company or customer data online
- Scareware
  - Floods the user with popup messages about a threat detected
  - Offers to fix the problem for a fee
- RaaS – Ransomware as a Service

Defenses

Ransomware Defenses

- Before the Fact (how is it getting in)
  - Vulnerability – Patch it
    - Follow your patching standards
    - Good vendor management
  - Bad IT Hygiene – Better security configuration
    - Mis-configured cloud product
    - Outdated encryption
  - Social Engineering – Security Awareness Training
    - Good web and email filtering

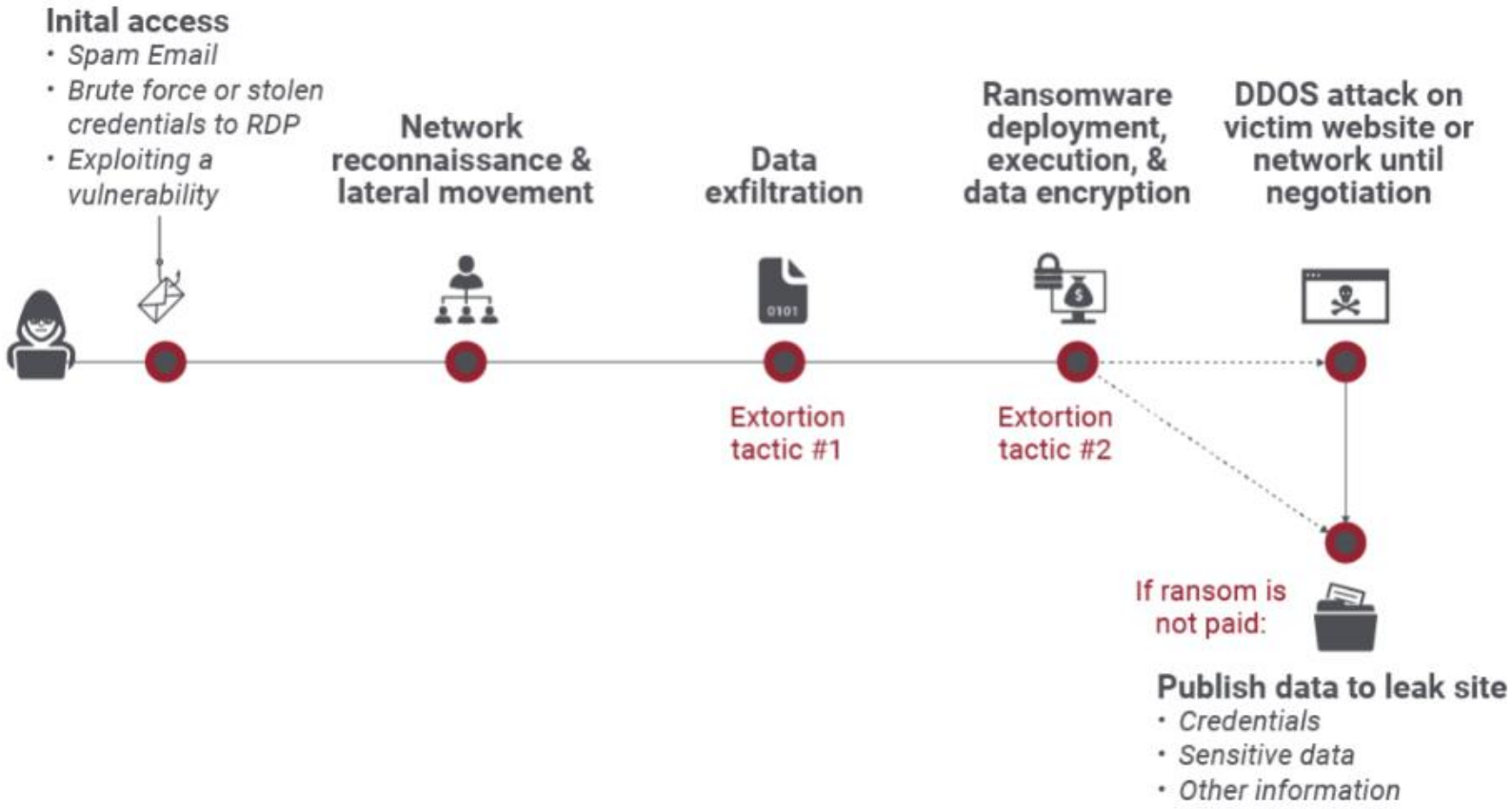
Ransomware Defenses

- After the Fact (already a victim)
  - Backups (*)
    - Offline so they are not affected
  - Incident Response Plan
    - Practice and Update
  - To Pay or Not to Pay
    - Decide before you need to decide

Ransomware Types (*) edition

- Double Extortion
  - Takes backups away to avoid paying
  - Puts greater pressure on stopping the attacker before they get in
  - You could be forced to pay twice
    - Once to unlock your systems / data
    - Once to keep data from being sold on dark web / released to the public

Ransomware Types (*) edition



Email Account Takeover

Bad Start to the Day

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

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 – known passwords from another breach
- Malware – Keylogger
- Poor Password Habits

Business Email Compromise

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.

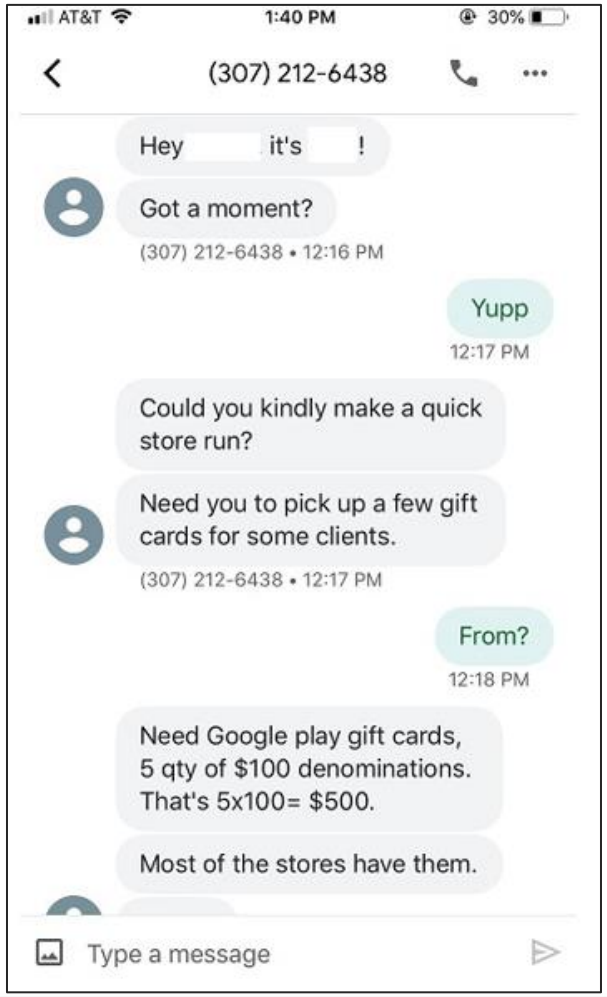
I will need you to make a wire payment today in the form of a deposit for the acquisition. Use this email as my full approval for this and any additional wires that may be required in the coming days.

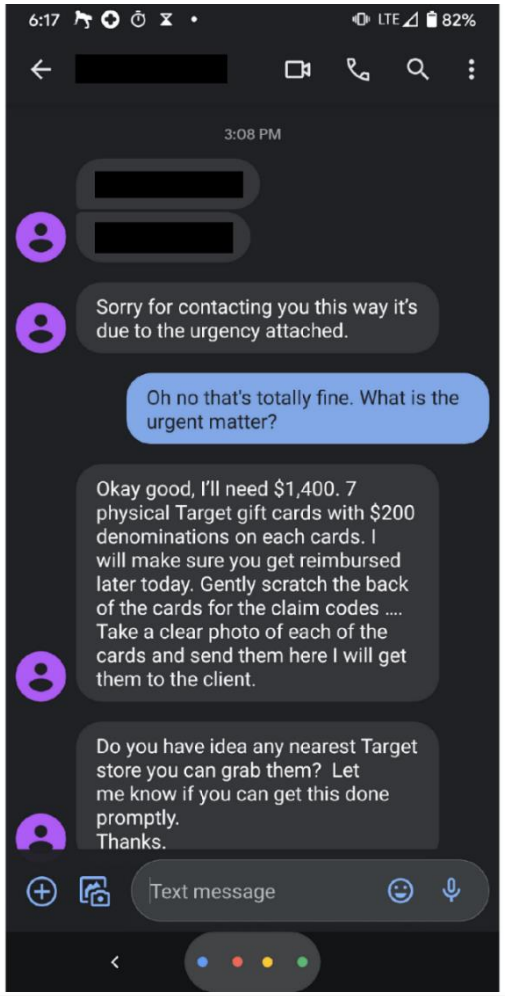
It's been agreed that, at this stage, the acquisition needs to remain private, so I have arranged for the lead attorney, John Jones, to contact you directly. He will work with you to ensure we have everything completed in line with the terms agreed.

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

Regards

Text Message from CEO?





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
  - Can be Text Messages or Phone Call

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

What is Business Email Compromise?

- 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

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
  - Have Your Own Email Domain

Defense - Better Passphrase Habits

- Passphrase - Protection with Mandatory Parameters
  - Enforced by the system – not manual
  - Three Strike Lockout Rule
  - Use complex passphrases - not dictionary-based passwords
  - Unique to each system – use a passphrase manager
  - Change or disable default accounts
  - ON ALL SYSTEMS

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

Questions

Contact Information

- Michael Bechtel
- Information Security Analyst
- mbechtel@vfccu.org
- Toll-Free (800) 622-7494 ext. 1101
- Website: www.vfccu.org/solutions_mobile/risk_management.html