CATO Security Awareness for Business and Municipal Accounts

Derek Boczenowski | Sr. IT Security Analyst | dboczenowski@CompassITC.com

Agenda

COMPASS IT Compliance

- What is Corporate Account Take Over
- Business Email Compromise
- Who is affected
- Cyber-Threats
- Security Approach
- Security Threats and Countermeasures
- Home Computer Use
- Tools/Resources/References
- Questions

What is Corporate Account Take Over?

COMPASS IT Compliance

1. Form of Corporate Identity Theft
2. Business' online credentials are stolen by malware
3. Criminal Entities initiate fraudulent banking activity
4. The Corporate customers' credentials are compromised
5. Money is transferred via wire or ACH transactions
6. Little or no ability to recover the losses

Business Email Compromise – The Latest CATO Threat

COMPASS IT Compliance

- Compromise of legitimate business e-mail accounts through social engineering or computer intrusion techniques.
- Conducts unauthorized transfers of funds
- Wire Transfers are the most common method
- From 10/2013 through 5/2016:
  - 15,668 U.S. Victims across all channels
  - Total Dollar loss: $1,053,849,635
  - 1300% increase since January of 2015

Business Email Compromise – Characteristics

COMPASS IT Compliance

- Businesses and associated personnel using open source e-mail accounts are predominantly targeted.
- Individuals responsible for handling wire transfers within a specific business are targeted.
- Spoofed e-mails very closely mimic a legitimate e-mail request.
- Hacked e-mails often occur with a personal e-mail account.
- Fraudulent e-mail requests for a wire transfer are well-worded, specific to the business being victimized, and do not raise suspicions to the legitimacy of the request.

Business Email Compromise – Characteristics

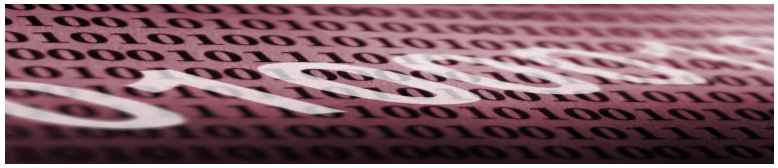
COMPASS IT Compliance

- The phrases “code to admin expenses” or “urgent wire transfer” were reported by victims in some of the fraudulent e-mail requests.
- The amount of the fraudulent wire transfer request is business-specific; therefore, dollar amounts requested are similar to normal business transaction amounts so as to not raise doubt.
- Fraudulent e-mails received have coincided with business travel dates for executives whose e-mails were spoofed.
- Victims report that IP addresses frequently trace back to free domain registrars.

Who is Affected?

COMPASS IT Compliance

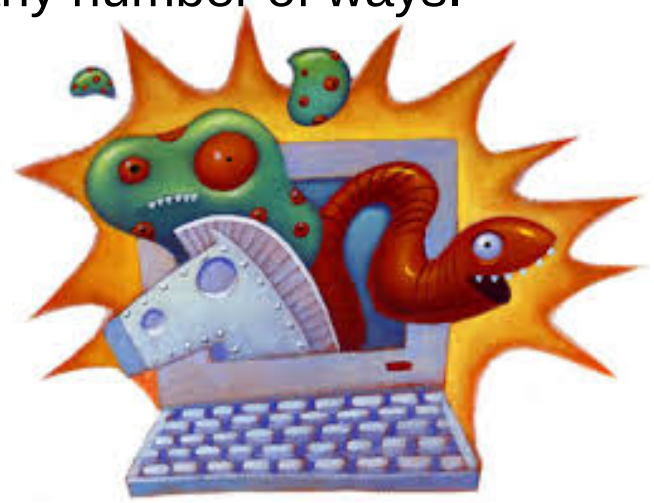
1. Potential Targets Include:
   a. Municipalities, school districts, large non-profit organizations
   b. Corporate businesses
   c. Any customers that perform electronic transfers
2. Losses range from tens of thousands to millions of Dollars
3. These thefts have affected both large and small banks



Cyber-Threats

COMPASS IT Compliance

1. The threats to businesses today are many and varied. Malware can find its way onto computers in any number of ways.
    a. Drive-by downloading
    b. Email-phishing
    c. Social Engineering
    d. Hacking/Exploiting weaknesses
    e. Virus and Worm infections



2. Many SMBs do not have the resources or expertise to protect their computer systems from the majority of these attacks.

Security Approach

COMPASS IT Compliance

1. How does Belmont Savings Bank, protect their customers?
   - Security Awareness
     i. Educate Employees about the threats and dangers out in the wild.
     ii. Publish Security Policies and Guidelines in regards to Wire and ACH transaction controls (dual-authorization)
     iii. Stay on-top of current threats and trends in security
   - Enforce Sound Wire/ACH Policies/Procedures
     I. Computer Base Enrollment – One Time Passcode
     II. Different Roles for Customer employees
     III. Daily Limits for Wires and ACH Transactions
     IV. Token-based Transaction Approval
     V. Dual-Control for Transaction Approval will be required
     VI. ACH and Wire Limits are reviewed based on transaction history
     VII. Requests for limit changes via email are verified by a call back to the customer number on file.

Security Approach

COMPASS IT Compliance

What Can our Customers Do to Protect Themselves?

Most Importantly Do **Something**.

1. Security Awareness Training
2. Antivirus/Antimalware Software
3. Perimeter Defenses
4. Appropriate User Access Control
5. Current Hardware/Software
6. Patch Management
7. Documentation

Security Threats and Countermeasures

COMPASS IT Compliance

- Malicious software: viruses
  - Malicious code embedded in e-mail messages or websites that are capable of inflicting a great deal of damage and causing extensive frustration
    - Stealing files containing personal information
    - Sending emails from your account
    - Rendering your computer unusable
    - Removing files from your computer
- What you can do
  - Do not open attachments to e-mails:
    - Received from unknown individuals
    - That in any way appear suspicious
  - If uncertain, contact professional IT assistance
  - Report all suspicious e-mails to a professional IT expert

Security Threats and Countermeasures

COMPASS IT Compliance

- Malicious software: spyware
  - Any technology that aids in gathering information about you or the credit union without their knowledge and consent.
    - Programming that is put in a computer to secretly gather information about the user and relay it to advertisers or other interested parties.
    - Cookies are used to store information about you on your own computer.
      - If a Web site stores information about you in a cookie of which you are unaware, the cookie is considered a form of spyware.
    - Spyware exposure can be caused by a software virus or as a result of installing a new program.

- What you can do
  - Do not click on options in deceptive / suspicious pop-up windows.
  - Do not install any software you do not need on your business computers
  - If you experience slowness / poor computer performance or excessive occurrences of pop-up windows, seek professional IT assistance.

Security Threats and Countermeasures

COMPASS IT Compliance

- Phishing
  - An online scam whereby emails are sent by criminals who seek to steal your identity, rob your bank account, or take over your computer
- What you can do
  - Use the “stop-look-call” technique:
    - Stop: Do not react to phishing ploys consisting of “upsetting” or “exciting” information
    - Look: Look closely at the claims in the email, and carefully review all links and Web addresses
    - Call: Do not reply to e-mails requesting you to confirm account information; call or email the company in question to verify if the email is legitimate
  - Never email personal information
    - When submitting personal / confidential information via a Web site, confirm the security lock is displayed in the browser
  - Review credit card and bank account statements for suspicious activity

  - Report suspicious activity to your Bank representative immediately.

Home Computer/Laptop Use

COMPASS IT Compliance

- Specific conditions and procedures should be followed when using home/laptop computers for business purposes
  - Any remote access to the corporate network/services should be through a secure VPN connection
  - Never use a business computer for personal use
  - Never allow anyone else to use your business computer
  - Home/laptop computers should have a personal firewall installed
  - Home/laptop computers should have antivirus and antispyware installed.
  - Laptop computers with confidential information should have hard drive encryption installed

Tools/Resources/References

COMPASS IT Compliance

1. NACHA – What is Corporate Account Takeover
   https://www.nacha.org/content/corporate-account-takeover-resource-center

   Conference of State Bank Supervisors – What is Corporate Account Takeover

   http://www.csbs.org/ec/cato/Pages/whatiscato.aspx

2. NACHA – Sound Business Practices for mitigating Risk of Corporate Account Takeover
   a) For Financial Institutions: - https://www.nacha.org/sites/default/files/files/Sound%20Business%20Practices%20WP.pdf
   b) For Businesses - https://www.nacha.org/sites/default/files/files/CAT%20-%20B.pdf

3. Conference of State Bank Supervisors: Tools and Resources
   http://www.csbs.org/ec/cato/Pages/catotools.aspx

4. BankInfoSecurity
   http://www.bankinfosecurity.com/interviews/ken-baylor-i-1753

5. Darkreading
   http://www.darkreading.com/smb/lawsuits-bring-clarity-to-smbs-in-corpor/240153406

6. Krebs on Security
   http://krebsonsecurity.com/

Questions?

COMPASS
IT Compliance

Derek Boczenowski

Compass IT Compliance, LLC

401-353-3024

dboczenowski@compassitc.com