RESOURCE BANK

Corporate Account Takeover (CATO) & Fraudulent Transactions

2024 Training

Introduction

- Resource Bank is committed to providing our commercial clients with a **highly sophisticated** level of online protection.
- Unfortunately, in today's digital age, **fraud** is a fact of life.
- All bank departments keep the security of your information in the **highest regard**.
- Our efforts in combination with your **diligence** will set you up for success in preventing a CATO event.

What is Corporate Account Takeover? (CATO)

- Cyber-thieves gain access to a business' bank account in order to **steal** online banking information relating to the business.
- Some thieves will also **change** information related to the business such as phone numbers and email addresses.
- The information the thieves are after can be obvious like account numbers and balances.
- Less obvious information would be the transaction history. The transaction history provides information such as: other financial institutions the business banks with, payroll company, common vendors and typical cash flow.

Common Attacks

- The most common technique is **malware**.
  - The malware infects a business' computers & laptops.
  - This happens through infected **attachments** or **links** via e-mail, websites, social media platforms, and even company networks.
  - If the links or attachments are clicked, the malware can install & provide the perpetrator with sensitive banking information such as account numbers and balances.

Common Attacks

- Social Engineering
  - Is used to deceive people into giving away sensitive information or performing actions that are not in their best interest.
  - This is a type of cyber attack that uses psychological manipulation to gain the victim's trust and break security practices.
  - Social Engineering can be a mix of communication methods including email and phone calls.

Why are Businesses Targeted?

1. They can initiate funds transfers via online banking.
2. Not as many **technological** resources to protect against fraud in smaller businesses such as systems that incorporate regularly monitoring accounts.
3. Additional protections for log-in's (password generation, two-step authentication, etc.).
4. Small businesses usually bank with a **wide array** of financial institutions that may not require these protection services.

How Can Financial Institutions Help?

- ❑Integrate **multi-factor** authentication for business accounts.
- ❑Require clients utilize **dual control** (transaction origination & authorization).
- ❑Initiate “out-of-band” confirmations on specific payment types (refers to text, email alerts, etc.).
- ❑Arrange “out-of-band” alerts for uncommon activities.
- ❑Prohibiting credential sharing.
- ❑Authorize & control exposure relating to the clients’ activities.

How Businesses Can Prevent Fraud

- ❑Utilize **dual control** for payments.
    a) Have one person authorize creation and one authorize release of payment.
- ❑Confirm that all security & anti-virus software on company computers & laptops are up-to-date.
- ❑Prohibit shared access
- ❑Second day verification by an employee not involved in initial transaction to prevent internal fraud.
- ❑Limit the functions of each computer & laptop **strictly** used for online banking
    a) Have a computer for general use that is not connected to internal network.
- ❑ Reconcile banking activity on a **daily** basis.
- ❑Incorporate alerts for unusual activity.

What is Business Email Compromise?

- **Business email compromise** (BEC) is the largest type of Corporate Account Takeover nationally for the last two years.
- This occurs when fraudsters, also known as “bad actors,” hack into a business’ email to attempt to reroute funds being sent electronically.
- Typically, there is a slight **variation** made to the email address that is usually undetected by the customer. Sometimes it may only be one letter!
- It is important to identify red flags and incorporate best practices.

Red Flags and Best Practices

❑Red Flags

a) Bad actor pretending to be the vendor or an employee and applies **pressure** to receive payment faster than originally stated.

b) Bad actor changes payment method from check to ACH or from ACH to wire.

c) All communication is being sent via email or fax without verbal verification.

❑Best Practices

a) Any time payment methods or payment information is changed via written communication, a callback should be made to the vendor **directly** with the current contact information already on file with your company.

b) When performing the callback verification, not only confirm the payment method but also that the payment account information is still valid.

If a Client is a Fraud Victim

1. Reach out to relevant law enforcement immediately.
2. Contact **Resource Bank** to initiate an investigation with receiving bank to determine if funds are recoverable.
3. Resource Bank will file appropriate paperwork and keep you informed of the claim status.
4. Take additional steps to evaluate anti virus software is up-to-date on company computers & consider bringing in an outside firm to address and correct any system compromises.

Additional Resources

- FFIEC

http://www.ffiec.gov/pdf/authentication_guidance.pdf

- FDIC

https://www.fdic.gov/

- FBI

https://www.fbi.gov/contact-us/field-offices

- FTC

http://ftc.gov/redflagsrule

- Internet Crime Complaint Center

http://www.ic3.gov/

- Financial Services

http://www.fsisac.com/

Questions?

CashManagement@resource.bank | 985.801.0120

Or send a secure message from within the online banking portal.

We appreciate your business and referrals.

RESOURCE BANK