2016 CATO & Information Security Awareness

Independent Bank

Member FDIC Equal Housing Lender

What is CATO?

CATO (corporate account takeover):

Is a form of corporate identity theft where cyber thieves steal a business' valid online banking credentials and use those credentials to initiate electronic funds transfers from the account(s).

Cyber thieves employ various methods to steal online banking credentials including the following:

- Mimicking an institution's website so an online banking user will enter his/her login credentials
- Using Malware to compromise a computer's security to obtain login credentials
- Using Social Engineering to defraud online banking users into revealing login credentials or other sensitive data

Malware (malicious software) can be a computer virus, worm, trojan horse, spyware, dishonest adware, crimeware, rootkit, or any other unwanted software.

Examples of CATO

A business' computer security may be compromised by an authorized online banking user performing one of the following actions:

1. Receiving & opening an **Email Attachment** infected with malware.
2. Receiving & clicking on an **Email Link** infected with malware.
3. Visiting a **Social Networking Website** & clicking on an **Ad/Video/Photo** infected with malware.
4. Inserting a **Flash Drive** infected from another computer with malware.

In each case, cyber thieves exploit the compromised computer system to obtain valid online banking login credentials. The criminal can then use the stolen credentials to initiate electronic funds transfers to the bank accounts of their criminal associates where the funds are withdrawn.

Electronic funds transfers methods include Domestic Wires, International Wires, ACH Vendor Payments, and ACH Payroll Payments.

Information Security Awareness

Basic Security Standards:

- ✓ Secure your computer & networks
- ✓ Keep passwords secure
- ✓ Limit administrative rights on your computer
- ✓ Install & maintain anti-virus/malware detection software
- ✓ Install & maintain spam filters for email
- ✓ Surf the internet carefully
- ✓ Install routers & firewalls to prevent unauthorized access to your network
- ✓ Install updates as available
- ✓ Block pop-ups
- ✓ Do not open suspicious emails or attachments
- ✓ Do not click on suspicious links
- ✓ Do not use public internet points
- ✓ Reconcile bank accounts daily
- ✓ Address any changes in your computer's performance (speed, rebooting, lock ups, etc.)
- ✓ Know how and to whom to report suspicious activity within your company and to your bank

Information Security Awareness

Layered Security Approach:

- ✓ Monitor IP Addresses
- ✓ Activate New User Controls – Administrator
- ✓ Use Dual Control/Approval Features
- ✓ Use out of band confirmations for transactions
- ✓ Use Secure Browser
- ✓ Apply pattern recognition software

New Threat

Business Email Compromise (BEC), Imposter Fraud, or Spear-Phishing/Whale-Phishing

In BEC, Imposter Fraud, or Spear-Phishing, a fraudster composes a fraudulent email request masquerading as a senior level officer of the company such as a CEO or CFO. The email will typically have one of two types of instructions for a junior level or data entry level employee.

1. The instructions may request the employee send a Wire for the purchase of a new company (merger/acquisition) which is confidential and should not be discussed openly among other employees.
2. The instructions may request an update to a vendor's ACH payment instructions or the addition of a new vendor's ACH payment instructions.

The junior level employee enters the transaction's instructions into online banking, may even have another mid-level employee approve the transaction in a dual control environment, and sends to the bank as fully authorized and authentic – even during a call back verification. In this type of fraud, the business helps conduct the fraudulent transaction.

Important: Always use a second verification process for every type of email instruction such as making a phone call to verify with the CEO, CFO, or Vendor.

Questions?

- Call or visit your local branch
- Contact a Treasury Management Representative
- Submit our Contact Us form online at www.ibtx.com