First American Bank

Ca$hTrac

Security Awareness - Overview

This guide was derived from a joint effort between the Federal Bureau of Investigation (FBI), the Financial Services Information Sharing and Analysis Center (FS-ISAC), NACHA - the Electronic Payments Association, and other Federal government agencies.

BACKGROUND

There has been a shift in the online criminal world from primarily targeting of individuals to increased targeting of corporations- In the past 12-months financial institutions, security companies, the media and law enforcement agencies are all reporting a significant increase in funds transfer fraud involving the exploitation of valid online banking credentials belonging to small and medium sized businesses. Eastern European organized crimes groups are believed to be predominantly responsible for the activities that are also employing witting and unwitting accomplices in the United States (money mules) to receive, cash and forward payments from thousands to millions of dollars to overseas locations via popular money and wire transfer services.

COMPROMISE OF THE CUSTOMER

Typically compromise of the customer is carried out via a "spear-phishing" e-mail which directly names the recipient correctly and contains either an infected file or a link to an infectious Website. The e-mail recipient is generally a person within a company who can initiate funds transfers or payments on behalf of the business. Once the user opens the attachment, or clicks the link to open the Website, malware is installed on the user's computer which usually consists of a Trojan keystroke logger, which harvests the user's corporate online banking credentials. Many types of spear-phishing have been used by criminal groups including messages impersonating the Better Business Bureau, U.S. Court System, and UPS to name a few.

THE FRAUD

The customer's online credentials are either uploaded to a website from where the fraudster can later download them, or, if the bank and customer are using two factor authentication system, the Trojan keystroke logger may detect this and immediately send an instant message to the fraudster alerting them of the secure web activity. The fraudster then accesses the financial institution through use of the captured username and password or through hijacking the secure web session.

The fraud is carried out when the fraudster creates another user account from the stolen credentials or directly initiates a funds transfer masquerading as the legitimate user. These transfers have occurred through wire or ACH that are directed to the bank accounts of willing or unwitting individuals. Often within a couple days, or even hours of recruiting money mules and opening accounts, money is deposited and the mule is directed to immediately forward a portion of the money to subjects in Eastern Europe by various means.

CUSTOMER RISK OF LOSS

1. If a hacker takes over one or more of my computers at work or a computer at home or via an internet café thereby learning my user credentials which results in the transfer of funds out of my company's business accounts, will the bank reimburse me?

   No, per your cash management account agreement, you are responsible for the security and integrity of the computers/networks used to access your account information at First American Bank.

2. I leave my digipass or passwords so that they can be shared in our office. I believe that they were used inappropriately by either one of my employees or a contractor. Will the bank reimburse me for these funds that were transferred out?

   No, per your cash management account agreement, you are responsible for employing sound internal control and information security best practices to safe guard access to the authorities and entitlements provided thru our system. You must be the gatekeeper over those aspects that you are closest and have custody for.

3. I would like the ability to enter a wire such that it does not require another approval in the process or I would like to grant powers such that my admin can both enter and approve wire transfers. Why should I not pursue this alternative?

   By pursuing this posture, you would not be following a best practice of establishing dual control whereby a different individual from the initiator must approve the transaction.

BUT I HAVE ANTI-VIRUS RUNNING….

1. How does malware infect my computer?

   Malware is introduced most commonly from spear-phishing emails or by visiting web sites. Sometimes malware infection is caused by attaching usb, cd roms, floppy disks or other removable media that is infected.

2. Won't anti-malware or anti-virus on my desktop stop the infection? How does it avoid detection?

   Anti-malware and anti-virus solutions are typically based on identifying the infection due to a 'signature' contained in their database. Often they spread so quickly in their polymorphic altered versions that the signature is not current enough. In addition, mail and mail attachment scanning should be preformed on the server prior to the mail ever arriving in your 'in-box'.

3. Should I just forget about using anti-malware or anti-virus solutions at all?

   No, these are good solutions, however, they are less effective against zero day attacks where the malware/virus is in a new or never previously identified form. By following the best practice described below, you can mitigate the risk of a zero day attack.

4. What can I do to make sure that my business account information and my funds cannot be touched by a perpetrator?

   Install a dedicated computer to be used only for cash management purposes without any email access, restricted to only access First American Bank's website, and lock down the computer by installing a PC firewall, anti-virus software and anti-malware software.

BROAD RECOMMENDATIONS TO BUSINESS AND CORPORATE CUSTOMERS

Your approach to safeguarding your customer information and financial assets consists of a matrix of compensating controls and control points that all complement each other. The controls on your side work hand in hand with the controls on our side to restrict access to your funds to only appropriate parties. These control points include:

- Account Controls:
  - o Educating customers proactively about account features that may protect their accounts, such as check cashing limitations and automated payment filters.
  - o **Recommend reconciliation of all banking transactions on a daily basis.**
  - o **It is recommended that you initiate ACH and wire transfer payments under dual control, with a transaction originator and a separate transaction authorizer.**
- Employ best practices to secure computer systems in your business, including but not limited to:
  - o **If possible, and in particular if you do high value or large numbers of online transactions, carry out all online banking activities from a stand-alone, hardened and completely locked down computer system from which e-mail and Web browsing are not possible.**
  - o Be suspicious of e-mails purporting to be from a financial institution, government department or other agency requesting account information, account verification or banking access credentials such as usernames, passwords, PIN codes and similar information.
  - o Opening file attachments or clicking on web links in suspicious emails could expose the system to malicious code that could hijack their computer.
  - o Install a dedicated, actively managed firewall, especially if they have a broadband or dedicated connection to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to a network and computers.
  - o Create a strong password with at least 10 characters that include a combination of mixed case letters, numbers and special characters.
  - o **Prohibit the use of "shared" usernames and passwords for online banking systems.**
  - o Use a different password for each website that is accessed.
  - o Change the password a few times each year.
  - o Never share username and password information for Online Services with third-party providers.
  - o Limit administrative rights on users' workstations to help prevent the inadvertent downloading of malware or other viruses.
  - o Install commercial anti-virus and desktop firewall software on all computer systems. Free software may not provide protection against the latest threats compared with an industry standard product.
  - o Ensure virus protection and security software are updated regularly.
  - o Ensure computers are patched regularly particularly operating system and key application with security patches. It may be possible to sign up for automatic updates for the operating system and many applications.
  - o **Consider installing spyware detection programs.**
  - o Recommend clearing the browser cache before starting an Online Banking session in order to eliminate copies of web pages that have been stored on the hard drive. How the cache is cleared will depend on the browser and version. This function is generally found in the browser's preferences menu.
  - o Verify use of a secure session (https not http) in the browser for all online banking.
  - o **Avoid using automatic login features that save usernames and passwords for online banking.**
  - o Never leave a computer unattended while using any online banking or investing service.
  - o Never access bank, brokerage or other financial services information at Internet cafes, public libraries, etc. Unauthorized software may have been installed to trap account number and sign-on information leaving you vulnerable to possible fraud.
  - o Familiarize yourself with First American Bank's account agreement and with your liability for fraud under the agreement and the Uniform Commercial Code as adopted in the jurisdiction.

- o Stay in touch with other businesses to share information regarding suspected fraud activity.
- o Immediately escalate any suspicious transactions to First American Bank particularly, ACH or wire transfers. There is a limited recovery window for these transactions and immediate escalation may prevent further loss by your business.

RECOMMENDATIONS FOR ONLINE FRAUD VICTIMS

In the event your business is a victim of fraud, there are a number of immediate recommendations you should take to help protect your financial interests. A few general suggestions include:

- Immediately cease all activity from computer systems that may be compromised. Unplug the Ethernet or cable modem connections to isolate the system from remote access.
- Immediately contact First American Bank so that the following actions may be taken as a priority to contain the incident:
  - o Online access to the accounts be disabled.
  - o Online Banking passwords changed.
  - o New account(s) opened as appropriate.
  - o Request First American Bank to review all recent transactions and electronic authorizations on the account.
  - o Additionally, ensure that no one has requested an address change, title change, PIN change or ordered new cards, checks or other account documents be sent to another address.
- Always file a police report with the local police department and provide the facts and circumstances surrounding the loss. Obtain a police report number with the date, time, department, location and officer's name taking the report or involved in the subsequent investigation. Having a police report on file will often facilitate dealing with insurance companies, banks, and other establishments that may be the recipient of fraudulent activity. The police report may initiate a law enforcement investigation into the loss with the goal of identifying, arresting and prosecuting the offender and possibly recovering losses.
- Maintain a written chronology of what happened, what was lost and the steps you took to report the incident to the various agencies, banks and firms impacted. Be sure to record the date, time, contact telephone number, person spoken to, and any relevant report or reference number and instructions.
- Realize that if you carry out personal online banking from the business computer system, there are also potential identity theft aspects to the compromise. Review the recommendation at the Federal Trade Commission's Identity Theft website.
- Dependent on law enforcement investigative and forensic considerations, it is recommended that you have your network and systems reviewed by a qualified computer forensic/information security professional.

INCIDENT REPORTING

Besides reporting the matter to local law enforcement agencies, the FS-ISAC strongly encourages victims of cyber crime to contact their local FBI field office, http://www.fbi.gov/contact/fo/fo.htm, or file a complaint online at www.IC3.gov.

INCIDENT REFERENCES

Further public reporting in relation to incidents believed associated with these matters are available below:

- "Clampi/Ligats/Ilomo Trojan: One of the largest and most professional thieving operations on the Internet," July 29, 2009, Joe Stewart, SecureWorks, Inc.
- "Fake Microsoft "critical update" spam propagating Trojan," June 22, 2009, Angela Moscaritolo, SC Magazine USA
- "Fraud Update: The 13 Hottest Schemes You Need to Prevent," May 26, 2009, Linda McGlasson, Managing Editor, Bank Info Security
- "How Hackers Snatch Real-Time Security ID Numbers," August 20, 2009, Saul Hansell, The New York Times
- "On the Backs Of Mules: An ACH Fraud Scheme," August 2009, Craig Priess, Bank Technology News
- "The Growing Threat to Business Banking Online," July 20, 2009, Brian Krebs, Washington Post
- "The Clampi Trojan: The Rise of Matryoshka Malware," July 30, 2009 Brian Krebs, Washington Post

For more information,
please visit our website at **www.FirstAmBank.com**
or call us at **847-952-3701**.

FIRST AMERICAN BANK