INSTITUTION FOR SAVINGS

BUILDING STRONGER COMMUNITIES TOGETHER SINCE 1820.

Online Security for Your Cash Management Account

The vast majority of cyber thefts begin with the thieves compromising the computer(s) of the business account holders. Perpetrators often monitor the customer's email messages and other activities for days or weeks prior to committing the crime. The corporate customer is most vulnerable just before a holiday when key employees are on vacation. Another risk period is on a day the business office is relocating or installing new computer equipment. Employees may be distracted and think a problem conducting online banking is due to a new network or equipment. Therefore it is important and necessary for the corporate customer's employees to follow established security practices. Basic practices to implement include:

1. Provide continuous communication and education to employees using online banking systems. Providing enhanced security awareness training will help ensure employees understand the security risks related to their duties;
2. Verify system users are currently employees and their access privileges align with their job responsibilities;
3. Work with IT consultants or dedicated IT staff to implement and maintain Network Segmentation;
4. Review and update network security including patch management and access privileges frequently;
5. Update anti-virus and anti-malware programs frequently;
6. Update, on a regular basis, all computer software to protect against new security vulnerabilities (patch management practices);
7. Communicate to employees that passwords should be strong and should not be stored on the device used to access online banking;
8. Adhere to dual control procedures;
9. Use separate devices to originate and transmit wire/ACH instructions;
10. Transmit wire transfer and ACH instructions via a dedicated and isolated device;
11. Practice ongoing account monitoring and reconciliation, especially near the end of the day;

12. Purchase Cyber Insurance to protect you against Cyber Crime Incidents;

13. Adopt advanced security measures by working with consultants or dedicated IT staff; and

14. Utilize resources provided by trade organizations and agencies that specialize in helping small businesses.

Red Flags of a Possible Takeover of a Business Account Include:

1. Configuration changes to cash management/online banking profiles:
    a. New user accounts added;
    b. New ACH batches or wire templates with new payees;
    c. Changes to personal information;
    d. Disabling or changing notifications; and
    e. Changes to the online account access profile;

2. Compromised internal systems used by employees resulting in:
    a. Inability to log into online banking system (thieves could be blocking the bank's access while they are making modifications to account settings);
    b. Dramatic loss of computer speed;
    c. Changes in the way web pages, graphics, text or icons appear;
    d. Computer lock up so the user is unable to perform any functions;
    e. Unexpected rebooting or restarting of computer;
    f. Unexpected request for a one time password (or token) in the middle of an online session;
    g. Unusual pop-up messages, such as "try back later" or "system is undergoing maintenance";
    h. New or unexpected toolbars and/or icons; and
    i. Inability to shut down or restart.

Examples of Deceptive Ways Criminals Contact Account Holders

1. The FDIC does **not** directly contact bank customers (especially related to ACH and Wire transactions, account suspension, or security alerts), nor does the FDIC request bank customers to install software upgrades. Such messages should be treated as fraudulent and the account holder should permanently delete them and not click on any links.

2. Messages or inquiries from the Internal Revenue Service, Better Business Bureau, NACHA, and almost any other organization asking the customer to install software, provide account information or access credentials is probably fraudulent and should be verified before any files are opened, software is installed, or information is provided.

3. Phone calls and text messages requesting sensitive information are likely fraudulent. If in doubt, account holders should contact the organization at the phone number the customer obtained from a different source (such as the number they have on file, that is on their most recent statement, or that is from the organization's website). Account holders should not call phone numbers (even with local prefixes) that are listed in the suspicious email or text message.

An Incident Response Plan for your Business

Since each business is unique, customers should write their own incident response plan. A general template would include:

1. Contact information for the bank;
2. Steps the account holder should consider to limit further unauthorized transactions, such as:
    a. Changing passwords;
    b. Disconnecting computers used for Internet banking; and
    c. Requesting a temporary hold on all other transactions until out-of-band confirmations can be made;
3. Information the account holder will provide to assist the bank in recovering their money;
4. Contacting their insurance carrier; and
5. Working with computer forensic specialists and law enforcement to review appropriate equipment.

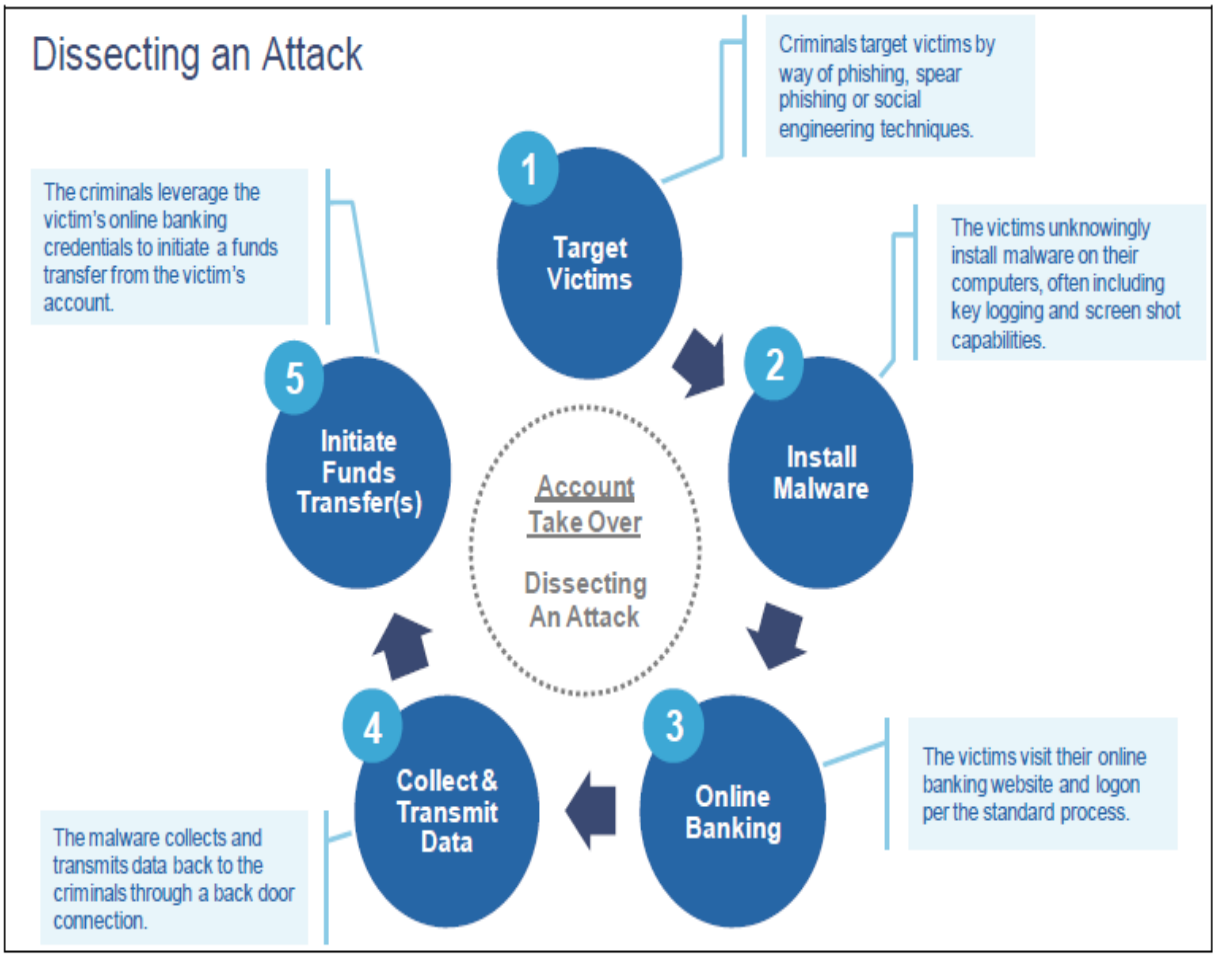

Figure 2: Dissecting An Account Take Over Attack