IS ANYTHING SAFE ANYMORE?

by Steve Brown

It used to be that using a password to protect information on the internet was good enough. Now, Georgia Tech researchers have just finished cracking 8 character passwords in about 2 hours. Powerful processors linked to hundreds of computers working together, have crushed the time it takes to crack a password. As such, these same researchers warn that any password less than 12 characters in length will soon be vulnerable. Perhaps that is a key reason the FBI, Secret Service and other agencies came out with a fraud advisory that banks might find useful to share with their business customers.

In the study, law enforcement begins by providing a decent outline of how criminals use malicious software ("malware") to steal personal information and log-in credentials of unsuspecting users. This is the type of data that can be used to steal money from bank accounts. These same criminals also use such access to steal customer lists and other proprietary information that can be used to cause indirect losses or reputational damage.

The above process, more generally known as corporate account takeover, has spread and criminals are now using it to target businesses, municipalities, non-profit organizations and others that transact business with banks. Being alert to the risk, having proper password protocols, maintaining open lines of communication with customers and being able to detect unusual activity can help protect both the customer and the bank.

To protect yourself and your customers, it is important to get into the mind of the criminal. Most often, they will use both technological and non-technological techniques to trick victims as a way to get personal information. Sending email attachments, accepting fake friend requests on social networks, using mass emails, pop up messages, career sites and scare tactics are all methods leveraged frequently. The whole goal is to get the person viewing the message to click on it, so using catch phrases such as "you have a problem with X" or a "complaint has been filed against you," or "you have been served a subpoena" are all disguises to achieve that magic click. Heck, these criminals even try to take advantage of current events by spamming people in areas where natural disasters have occurred, there are major sporting events or by using hyped celebrity news.

To prevent such attacks, start by spreading the word (and constantly reminding employees and customers) never to open attachments or click on links from unsolicited emails. Let everyone know that banks don't ask for account information, passwords, credit cards numbers or anything else like that in an email ever - period. To really protect yourself, consider having a separate computer entirely that is only used for online banking and nothing else. Then, turn the computer all the way off, turn off the wireless device and/or unplug connectivity when not in use.

Other things your customers and employees should be doing to protect themselves include: installing and maintaining spam filters; having up to date anti-virus software; frequently changing passwords; blocking pop-ups; encrypting sensitive folders; using two separate computers to initiate ACH and wire transfer payments; encouraging customers to set up texting, call backs or batch limits with your bank; reviewing all accounts regularly to detect unauthorized activity; checking your outbox for emails you did not send; regularly running virus and malware scans; and discouraging employees

from using public internet access points (such as open access airports, internet cafes, etc. when accessing personal information or accounts).

For those interested in reading the full report, follow the "Full Report" link in our "Related Links" section in the right column. In addition, for those interested in having a contingency plan after a compromise, follow the "Contingency Plan" link. Spread the word and help increase online safety for yourself, your employees and your customers

Related Links:
Full Report
Contingency Plan

BANK NEWS

Election Impact

The final tally with the midterm elections where in-line with market expectations. Given the Republicans have taken the House, the odds of maintaining a lower tax structure has increased to help banks, but the probability of lower rates has decreased. In addition, look for pressure after Jan to reopen both the healthcare debate and financial reform. While both may prove to be a good thing in the long run, the injection of uncertainty will hurt businesses, as they put off many investment decisions to see how the dust will settle. We predict the net impact of having a divided Congress is both positive and negative and will ultimately result in little change for the economy. Look for Rep. Spencer Bachus (R, AL) to get the chair of the powerful House Financial Services Committee.

Big Bonus

Several banks moved their new account bonus to $500 for the first time. Harris Bank will give its business customers $500 for opening an analyzed checking account and an additional $500 for using its remote deposit utility. HSBC gives away a $500 Apple gift card for those that open a premier banking relationship.

Unemployment

Moody's projects unemployment will fall to 8% by the end of 2011 and 7% by the end of 2012.