PCBB

BID Daily Newsletter

Mar 31, 2017

Customer Service Without A Smile

by Steve Brown

In case you haven't heard, a team of physicists have figured out how to encode data on single atoms. Using some super brains, super cool magnets and some super elbow grease they got it to work. By the way, an atom is about 1mm times smaller than a human hair, so this is really, really small. Pretty neat trick and it shows what one can do by attacking a problem head on.

Speaking of attacks, there is a new sort of cyberattack going on that bankers should know about. According to CIO, hackers call the customer service line at hotels or restaurants and pretend to be clients who can't access the online reservation system. The hackers also send an email to the customer service agent and it includes an attached word document that supposedly contains their reservation information. Unbeknownst to the customer service rep, the document is actually designed to download malware that steals customer credit card information.

While this particular crime wave doesn't appear to be targeting banks just yet, it is another reminder that when it comes to cybersecurity, a bank can never be too careful. Indeed, these latest attacks highlight how important it is to remain vigilant in the battles raging all over the place as bankers and other companies fight the cybersecurity war being waged against us.

We've written before that your employees are often the weakest link in this area so a focus here is critical. Consider a CEB study from late last year that found more than 90% of employees violate policies designed to prevent data breaches. The scary thing is that offenders aren't always taking aim at company systems maliciously. In most cases, problems occur unintentionally, such as an employee accidentally clicking on something they shouldn't, or cutting security corners to get the job done faster.

Bank leaders need to reinforce the message that controlling cyber risk and ensuring company security is everyone's business. Clear protocols should be regularly reviewed and updated. New breach events, such as the above regarding customer service infiltrations, necessitate tabletop testing, enhanced review and possible update of protocols with recommunication bank-wide.

To help engage employees and better understand their concerns, role playing can be an option. This sometimes helps employees gain insight first hand into potentially risky situations and the best ways to react calmly. Knowing that they can rely on their coworkers and management for guidance in such exercises creates not only a feeling of support, but also commitment.

Although most community banks know password sharing is a security no-no, this too remains an area to review regularly. Research finds about 70% of people use the same password for multiple websites, 62% of smartphone owners don't password protect their device, 31% of people have shared passwords with friends and people over and over again use dumb and easily broken passwords like "password," "iloveyou" and "abc123". To protect your bank, be sure employees have clear guidance about what they should and should not be doing here; help them understand the risk to themselves and the bank in using simple passwords all over the internet.

Some community banks may feel immune from trouble because of their size, but in reality, you have just as much to fear from hackers as the largest banks. While those names are more known worldwide, almost everyone knows all banks are listed in the FDIC, lists are everywhere and bank websites are easily found. No matter your sophistication here, a continual focus on cybersecurity is needed to avoid trouble.

BANK NEWS

M&A Activity

1) First Bank ($1.1B, NJ) will acquire Bucks County Bank ($198mm, PA) for about $27.2mm in stock (100%) or 1.24x tangible book. 2) Mid Penn Bank ($1.0B, PA) will acquire The Scottdale Bank & Trust Co ($263mm, PA) for about $59.1mm in cash (10%) and stock (90%) or about 1.30x tangible book.

Brand Consolidation

Synovus Financial Corp ($30B, GA) said it will collapse 28 locally branded banking divisions into the parent's name as it seeks to reduce customer confusion and increase awareness of broader capabilities.

Normal Economy

Fed SF President Williams has officially sounded the all-clear for the economy, saying the country has "largely attained the hard-sought recovery we've been after for the past nine years."

Cyber Concern

Cisco cybersecurity research finds security professionals cite the following as the biggest sources of concern related to cyber-attacks: mobile devices (58%), data in the public cloud (57%), cloud infrastructure (57%), and user behavior such as clicking malicious links in emails or websites (57%).

Higher Rates

Banks with floating rate loans should continue to outperform in coming years, as Fed officials again are out indicating the economic situation supports ongoing rate increases. Boston Fed President Rosengren said he believes 4 rate hikes this year would be appropriate, SF Fed President Williams said he wouldn't rule out more than 3 rate increases this year and Fed Vice Chair Fischer said he thinks 3 rate hikes this year seems about right.

Return Biz

Accenture research finds 75% of banking customers who have made a purchase from their bank would consider returning as a repeat customer.