Phone Hacked

by Steve Brown

This past August, a 12 year-old boy had what is sure to be the most memorable trip to a museum he will have in all his life. That's because the boy, who was visiting a Leonardo da Vinci-themed exhibit at Taipei's Huashan 1914 Creative Arts Center, tripped while touring the show and accidentally put his fist through a 350Y old painting. Luckily for the boy, the painting was insured and organizers of the exhibit have said they would not pursue restoration costs from his family. Although the boy's identity has not been released, a video of him falling into the painting was caught on closed caption cameras and later released by the museum so it has made the rounds of the Internet.

As crazy as this incident may seem, it is just one of several such museum incidents that have left famous works of art damaged or irreparably destroyed. Given how accessible and wide open most museum pieces are, it is actually surprising that more priceless works of art are not destroyed--particularly in an era where few people seem to do anything for long without repeatedly glancing at text messages or emails on their cell phones and not paying attention to the world around them.

This made us think about what else people are doing with their phones and more specifically as that might relate to banking. For example, consider the story about Apple's iPhone recently being hacked by thieves who stole the Apple accounts of more than 225,000 users.

In all fairness to Apple, following years of what was essentially a "free ride" for users who rarely had to deal with viruses; the massive popularity of its devices has spurred hackers to turn their attention to all things Apple. In this case, the cyber criminals actually took advantage of security weaknesses introduced by iPhone users who engaged in a practice known as "jail breaking." This process removes the restrictions of Apple's operating system in order to expand the phones' capabilities or include features service providers would otherwise charge extra for (usually used when playing difficult games).

By targeting "jail broken" phones, hackers successfully infected these devices with malware that allowed them to access the iTunes App Store information for each phone. This gave them the phone's individual ID number, account username and password. This was all information that enabled the hackers to prevent hijacked phone owners from recovering their phones. Oddly, even though iPhone users themselves were responsible for weakening the security system, the incident is a major publicity nightmare for Apple--especially since it occurred just before releases of the latest iPad, iPhone and Apple Watches.

Given the reality that customers are often the weakest link in any kind of security system, community banks should consider any and all ways that customers could potentially compromise the security your bank puts in place. People are always one if not the weakest link in the chain, so it is important to educate customers about the myriad of things they could do to potentially jeopardize the security of their accounts as you seek to protect the bank from human error.

One reminder that never goes out of fashion is to remind customers to do simple things such as making sure passwords are not easily cracked and don't contain obvious things such as the word "password." Customers should also incorporate other preventative measures such as regularly checking account balances, card activity and even credit reports for odd entries.

As customers continue to embrace more and more online and mobile banking applications it is important to continuously look for ways these programs could potentially be compromised and to educate users about possible pitfalls. Doing so is just another way your bank can demonstrate you are looking out for your customers' best interests.

BANK NEWS

Technology Changes

Deutsche Bank research finds banks now say 30% of IT budgets go towards "change the bank" costs and 70% to "run the bank costs."

Model Validation

In the crisis, regulators found out some models bankers were using did not hold up very well when bad things happen, leading to poor decision-making by some management teams. As a result, model risk management and validation requirements are all about testing and evaluating the models that could impact your bank or that you heavily rely upon to make decisions. Models need to pass muster if you are going to use them to make critical decisions, so one key area to look at closely is to look at your assumptions when you do such an evaluation. Then, do ongoing testing to be sure your models don't "drift" too far from reality no matter the market conditions.

IRR

An AuditOne survey of areas regulators flagged for material criticism in this area finds the following were the Top 7 cited by bankers: modeling assumptions (15%); level or structure of IRR limits (11%); range or selection of simulations run (7%); overall IRR exposure (7%); back testing of model results (6%); other (6%) and board or ALCO governance (5%).

Past Due/Nonaccrual

Under the new risk-weighted capital rules, loans that become past due 90 days or more or are nonaccrual are subject to a 150% risk-weighting requirement. One exception is for residential loans, which move from 50% to 100% in this case.

Rate Hikes

Cleveland Fed President Mester said she believes "the economy can handle an increase in the fed funds rate and that it is appropriate for monetary policy to take a step back from the emergency measure of zero interest rates."

Lending Shift

Wells Fargo says it plans to try and double the percentage of credit card loans it has on its books in the coming years as it seeks to boost ongoing performance.

Not Ready

The latest analysis by PaymentsSource finds about 75% of merchants have not yet converted to EMV chip payment processing systems.