Phishing And Farming

by Steve Brown

Psssst, crooks are trying to get into your bank's system to steal money from you and your customers. Well duh--like there is anything new about this! The skill of the defenders in the industry has improved, but the fraudsters have evolved as well. We wanted to pass along a few new developments from the fraudsters.

One of the most audacious methods happened in Brazil at an ATM; a customer put in his card and pin and asked for a printed balance. The transaction failed, the customer smelled a rat and called the cops. The police removed a fake machine face complete with screen and keypad that covered the entire ATM machine. There was a dissembled computer powered by batteries with a card skimming device complete with a 3G connection for transmitting the card information to the waiting recipients. It's a little hard to imagine someone walking up to an ATM machine and installing an entire new machine on top of the old without anyone asking a question, but stranger things have happened. As in so many scam attempts, what alerted the bank customer to call police was a misspelled word on the screen. It would seem the crooks didn't spend their education efforts on perfecting their grammar.

Beyond the fake ATM machine, standard phishing attempts abound and rely upon social engineering to convince customers to reveal their data. Customers often don't understand authentic website validation like the picture of a cute puppy when you log in. Bank web sites can go overboard requiring the answer to numerous questions before logging in, resulting in customer frustration. Nonetheless some kind of multifactor authentication is necessary, and education of customers on the necessity for authentication and on how to watch for it is time well spent.

The majority of fraud comes from customer PCs, primarily through the takeover of online bank accounts. This is a change from a few years ago when almost all fraud originated from credit card numbers. Customers have become more sensitive to standard ploys used to take user credentials, but once again, more imaginative means are becoming common. In addition, people sometimes don't think about risk. FDIC studies show that 60% of people will insert a thumb drive they find into their computer and 90% will do so if there is a company logo on it. Meanwhile, 41% share passwords with other people and 90% do so across accounts. Once in the account, thieves initiate ACH and wire transfers and the money is gone.

Pharming is something entirely different and is far more dangerous to your institution. Pharming targets provider infrastructure and can destroy confidence in your institution. This is because end-users are unaware of the problem until it has already happened. That leaves the only responsible party as your institution or your service provider, as no customer error is involved. Here, the FDIC is concerned enough to have issued guidance on the subject both concerning third party risk and due diligence, as well as guidance for internal controls. Pharming comes in a number of flavors--it may alter your website, or reroute traffic from your web site elsewhere such as to a fraudulent web site, or there may be a "man in the middle" which allows a hacker to monitor online customer sessions.

By whatever means, there are people out there trying to take your money because that is where the money is--banks. The best bet is still to educate your staff and your customers, stay up to date, beef up security and hopefully drive the fraudsters to look for an easier target.

BANK NEWS

Loan Opportunity

The latest Wells Fargo/Gallup Small Business Index finds small business owner optimism has now reached a 5Y high. Cash flows are up and 48% of owners project strong sales this year.

Settlement

JPMorgan Chase will pay $614mm to settle claims it improperly approved FHA and VA loans that did not meet underwriting guidelines.

Fed

Speeches from FOMC officials recently indicate the $10B taper removal pace will continue despite market volatility and low short rates are likely to continue through this year.

Cost Cutting

A PWC survey of CEOs at major companies worldwide finds 76% have cut costs in the last 12 months and 64% plan to do so over the next 12 months. Meanwhile, other areas CEOs say they plan implement include: implementing a cost-reduction initiative (64%), outsourcing a business process or function (25%) and in-sourcing a previously outsourced business process or function (14%).

Capital Standards

Fed Governor Tarullo said he expects the final capital leverage rule for U.S. banks will incorporate a recent international Basel III calculation revision. If so, the move will toughen regulations and limit debt funding.

Consent Order

The FDIC and OCC have issued a consent order against bank vendor and technology service provider FUNDTech. Under the order, FUNDTech must have: an internal auditor or integrated risk-focused audit program, formalized policies and procedures to handle vendor risk, an enterprise wide risk assessment, business continuity planning, patch management procedures, an effective log review to detect, identify and act on potential threats and other components. FUNDTech develops transaction banking solutions including payments and liquidity management; cash management, financial messaging through the world's largest SWIFT service bureau, electronic invoice presentment and trade services; remote deposit capture; merchant services and mobile banking.