Pestilence

by Steve Brown

We had to smile at a recent report that the Midtown NYC offices of investment management behemoth PIMCO had been invaded and besieged by bedbugs. Were employees sleeping on the job? Was it the result of long forgotten gym bags stuffed under desks? As with any pestilence, it's far less amusing for the victim, so we won't make too much fun of PIMCO as it could happen anywhere. For those seeking more facts, bedbugs have plagued humans for more than 3,300Ys.

Pestilence comes in many forms and as awful as bed bugs may be, the perpetrators of bank fraud may be even more difficult to detect and eradicate. We all know that most modern bank fraud happens by electronic means. There are cases where hackers find their way into corporate computers and generate wire or ACH transfers. Smaller businesses, municipalities and school districts are often targets because they often hold large bank balances and have less robust security than larger organizations.

Individuals are often targets as well. In the past such fraud was easy to spot as it mostly came from hapless innocents answering the call of deposed Third World monarchs needing a little help with transferring funds. Unfortunately, most email fraud these days is far more sophisticated. One technique that has come to light recently uses a hacked email account. In one scam shared with us by some astute bankers, the hacker looks through old emails after compromising a customer email account and looks for a bank generated email. The crook then responds to that email changing the subject line to "wire request". The message from the "customer" explains that he/she is away from their office, or traveling in order to circumvent the callback process that the bank requires. The email message pressures employees feigning either irritation or desperation because they are "traveling and need money" due either to injury or robbery. The intent is to find a bank employee that mistakenly will ignore normal protocols in order to service a seemingly desperate customer in need.

Most banks probably think they wouldn't allow that one to get through, but how about this scenario: The wire request email comes to the bank's CCO or CFO or someone else in senior management and outside the normal loop for transaction protocols. The senior manager forwards the email to an appropriate ops person, asking them to handle it. The ops person assumes there has been personal contact made by the CCO/CFO and completes a wire transfer form complete with account number which is then emailed back to the "customer." The hacker occupying the customer's email account now has everything needed to cause real damage. While most banks have restrictions on emailing anything with customer account numbers, the bigger problem here was skipping the step of ascertaining customer contact, because the original request was sent to the CCO/CFO. Most banks have officers' names on their web sites, and it's not too hard to guess standard email address formulas in order to pull this off.

Our final example for today was a wire transfer request from China on the account of a small manufacturer who did business in that country. This was not outside their normal pattern of business, but there was a misspelling in the email address. The bank ultimately found an additional initial or a similar variation in the domain name (like jbsmith.com instead of jsmith.com). Once again, the message stated the customer was traveling and in meetings in order to circumvent the normal

callback procedure. The bank's employees initially missed the changed email address, but called the customer and discovered the ruse.

To combat the bedbug issue, PIMCO moved employees to remote locations (are biting bug infestations a part of your bank's disaster preparedness plan?) while the offices were fumigated. For bankers seeking to thwart hackers and cyber theft, we suggest looking at human behavior and not insects. It usually comes down to human error. One very sharp insurance broker with hundreds of bank clients told us that about 99% of the time a problem occurs, it is because a bank employee doesn't follow stated protocols--which means the event is likely not insurable.

Community banking is all about delivering exceptional customer service, especially if customers are experiencing adverse circumstances. Just be certain employees make real contact with a real customer to protect your bank from an invasion of pests.

BANK NEWS

Mobile Checking

Aite Group estimates 37% of small businesses use a mobile device to check their bank balances.

Customer Access

A study by Youbiquity Finance finds bank customers now use 6.2 channels to interact with their banks vs. 4.3 just 2Ys ago - a 44% increase. Channels include branch, telephone, mobile, ATM, social media, web chat, video, email and others.

Cyber Security

Regulatory agencies have set industry standards for cybersecurity for companies including banks to adopt risk based, concurrent and continuous functions designed to identify, protect, detect, respond and recover from such risks. This is called the Framework Core according to the National Institute of Standards and Technology.

Cyber Protection

Governmental agencies and regulators indicate banks should identify and put protections in place around "critical infrastructure." Such infrastructure is defined as systems and assets, whether physical or virtual, so vital to your bank that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity or economic security of your bank.