KnowBe4.com
Human error. Conquered.

Financial Institutions Fall Victim To Cyber-Theft –
Could Internet Security Awareness Training Have Prevented The Larceny?

SITUATION
In a cyber-twist, a bank is targeted and (possibly a lot) more than $100K removed from its coffers. The bank won't say how much. Most of our case studies involve businesses who wake up one morning to find their bank accounts emptied of accumulated cash. This time a bank felt the sting of the cyber-gang. So for once it was not the small businessman that was hit but the bank itself. Makes you wonder how many other banks have found themselves the victim of cyber-theft. This is especially relevant when you hear about banks that for legal reasons are not able to take responsibility for their clients when they have been defrauded. There is irony in all of this, especially when you take into consideration a federal credit union.

CASE IN POINT – SALT LAKE CITY, UTAH MAY 20, 2010
The Treasury Credit Union is a financial facility servicing federal employees and the families of the U.S. Treasury Department in Utah. On a sunny Thursday in May, somewhere around 70 wire transfers were made from one of the bank's own accounts. The transfers were made at low increment amounts of under $5,000 to money mules for a total in the low six figures. Some of the money was returned.

How did the criminals infiltrate this supposedly well-protected financial institution? Just like they do any other business; a bank employee's login and password was stolen, by malicious software most likely via phishing and the Trojan horse was inserted into the computer. This was accomplished despite the fact that the computer and network was well-protected by an antivirus. The Trojan horse was not detected; no wonder when you consider the user went to the phishing site and literally invited the malware in. Last July, organized thieves used money mules to steal tens of thousands of dollars from Huntington, W.V. based First Sentry Bank.

DIGITAL CRIME OUTPACES REAL-WORLD ROBBERIES
Digital crime now outpaces real-world bank robberies in terms of losses. In 2009, there were 8,818 bank robberies netting criminals an average of $4,029 -- a total of about $35.5 million, according to the FBI's Uniform Crime Reporting (UCR) program. However, 60 percent of bank robbers were caught, often very quickly.

Compare that to fraud statistics of Automatic Clearing Houses (companies in charge of electronic funds transfers and credit card payment processing). The recent arrests connected with Zeus accounted for some 390 reported cases where $70 million was stolen from accounts. The criminals had attempted to steal some $220 million. The investigation mainly netted the lowest ranks of the criminal network -- the so-called money mules that remove stolen funds from their accounts and transfer the money to international accounts abroad. In general, the money mules are people who are duped into believing they are working for a legitimate company processing payments.

ANALYSIS
It just goes to show you that despite sophisticated security, the weak link even in a financial institution proved to be an employee. One of the keys to security is educating personnel on Internet Security Awareness. If the employee had been educated, a large amount of money would have been saved and much aggravation would have been avoided.

Digital crime now outpaces real-world bank robberies in terms of losses. In 2009, there were 8,818 bank robberies netting criminals an average of $4,029 -- a total of about $35.5 million, according to the FBI's Uniform Crime Reporting (UCR) program. However, 60 percent of bank robbers were caught, often very quickly.