

Beyond the Wild Wild West

Days of the Wild: I can see it now, a dusty man riding his horse, who is adorned in all black and a bandana over his face to conceal his identity, screaming “stick em up” in the bank lobby. However, the days of the wild, wild west are long over. Chances are this is not going to your neighborhood bank today. But the odds that you will be targeted in one way or another are very high.



I do not want to make light of the first situation but the fact of the matter is, banks have gotten better at protecting themselves. It is now the consumer that is a much easier target. This is due in large part that consumers lack awareness and training in what is being done today. These bad guys employ tactics designed to fool the average consumer.

Identity Theft: Identity theft is the fastest growing crime in America. In fact, almost 10 million Americans were victimized by this crime in 2004. It cost approximately \$5 billion dollars and this does not take into account time, effort, and the emotional expenses tied to these crimes.

What is Identity Theft? Bad guys have developed techniques in order to obtain private and personal information with the intentions of selling this information to unsavory third parties or to obtain fraudulent accounts in the victim’s name.

What do you look for? These bad guys often call unsuspecting victims by telephone pretending to be from the victim’s bank. They ask the victim to verify personal information like account numbers or social security numbers. No reputable bank will ask for this information over the telephone. If someone asks for this information, respectfully decline. Your bank has this information on file and will never ask for you to comprise personal private information.

Phishing: Phishing is a similar technique but uses e-mail instead of the telephone as a medium. Phishing is sending out millions of e-mails to perspective victims with a link to a fictitious website. The website is designed to look identical to a particular bank’s website in hopes that the victim will give up private information.

Phishing has become more sophisticated and targeted in recent years due to tools and methods that have been developed. This has been particularly effective for these scammers as up to 80% of those targeted often comprise personal information. It takes less time and effort to perpetrate and is very effective.

Again, no reputable bank is going to ask for private information in an e-mail. To protect yourself if you receive an e-mail such as this, close out of the e-mail and log on directly to your bank’s website. This ensures you are on the bank’s secure website and not that of a hacker’s.

What You Can Do: Times have changed. Unfortunately, there are bad people trying to take advantage of good people. But you do not have to take it. Shred letters with private information, do not reply to e-mails soliciting personal information, and do not give private or confidential information over the telephone. These simple steps will help anyone better protect themselves against the likes of these bad guys.

Consumers are urged to report the incidents to the Indiana Attorney General’s Fraud Division 800-382-5516 or online at www.in.gov/attorneygeneral.

Bobbette Fagel, CISA, CISM

Bobbette, Vice President of **infotex**, is a Certified Information Systems Auditor and Certified Information Security Manager, and has worked with Infotex since its inception. She has been intimately involved in compliance projects for financial organizations and hospitals, and leads our efforts on compliance program development as well as policy and procedure.