Security, Passwords And Hacking

by Steve Brown

The idea of hiding money at home is nothing new. This practice is said to be embraced by those who don't trust banks and who want to keep their cash nearby. The problem is, hiding cash in the home isn't usually safe given the multitude of potential disasters that can strike. Take the experience of Qi Shengli, a 60Y old farmer who lives in a small town in China. Instead of depositing his savings of 20,000 yuan ($3k) in a bank, Shengli divided his bills between two bags, which he buried in the ground within the corner of his bedroom. But when he recently dug that money back up Shengli discovered that termites had eaten a good portion of it. Though bankers were only able to piece together a small portion of his money, all was not lost. News of the situation caught the attention of a Beijing artist, who decided to pay Shengli the original value of his savings in exchange for the termite eaten bills. The artist plans to turn them into a piece of art to demonstrate the danger of storing money at home for China's elderly population in rural areas.

While the likelihood of termites infiltrating the monetary holdings of most banks is pretty much nonexistent, banks are not immune from the idea of feeling overly confident about security practices that are not necessarily impenetrable. A perfect example is the passwords used to secure the individual accounts of customers. According to the findings of a recent study conducted by the University of New Haven's Cyber Forensic Research, more than 33% of major banks have weaker password policies and enforcement practices than the majority of social networking platforms. Specifically, the study discovered that while all banks require users of online banking services to create passwords that contain a mixture of letters and symbols, six of the country's 17 largest banks still use security systems that do not require case sensitive passwords to protect these accounts. By depending on security systems that fail to differentiate between "JoHnDoE123" and "johndoe123," the accounts of individuals who use online services with these banks are significantly easier to hack into than those protected by case sensitive passwords.

While community banks were not included in the study, it should go without saying that the issue is one all banks should be aware of and act to correct if needed. It is critical to be sure password security efforts are strong. Of course, security concerns are by no means limited to password protection.

At the same time online hackers are becoming increasingly aggressive and sophisticated in their efforts to breach the sensitive records businesses store on their customers. These include credit card numbers, to account information and personal details such as social security numbers. Further, a growing number of businesses are beginning to use cloud storage for much of the information they maintain. It turns out, however, that the number of businesses around the world that use encryption to protect customer data is still relatively low, according to a study recently conducted by Ponemon. They found that while roughly 84% of companies in the world's 11 largest economies are gearing up

to use cloud storage for data by 2018, only 37% of these same companies are planning to use encryption to secure that data. While this survey was not unique to the banking industry, we figured community banks would still want to know about it, given that it is more than likely your customers will be impacted by the rise in online hacking.

Given the ever increasing sophistication of hackers' efforts, we would totally understand if many of you felt the urge to just climb into a hole to hide away from it all. But, as Qi Shengli learned the hard way, even that tactic may not be foolproof, so taking action on the security front is probably a better approach.

BANK NEWS

More Mobile

A Fed survey finds 43% of adults say they used their phone for financial activities vs. 39% back in 2014 - a 10% increase in 2Ys. At this pace, about 52% of people would be expected in 4Ys and almost 70% in 10Ys, so community bankers will have to continue to morph the business model to keep up with this change.

Housing Slowdown

Analysis by broker Knight Frank LLP finds luxury home prices in 10 global cities are expected to be 1.7% this year vs. 3.0% in 2015. While still higher, this would mark a 43% decline YOY.

Bond Slowdown

JP Morgan research projects fixed income trading activity will decline 40% YOY in Q1.

Mobile Alerts

A Fed survey finds more than 50% of mobile banking users say they get push notifications, text messages or email alerts from their financial institution.

Human Mistakes

Deloitte research finds more than 95% of cyber breaches are a result of user (human) errors such as clicking on fake links, opening malware websites or using weak passwords.

Email Compromise

The FBI indicates it has seen a 270% jump in victims and losses due to business email compromise. The most typical version is an urgent email to the CFO to wire money reportedly from the CEO who is too busy to be bothered and needs the money wired out quickly or for other sensitive information to be sent. The FBI reports that from Oct 2013 to Feb 2016, there have been 17,642 victims and $2.3B in losses reported.