Recent Internet Crime Report Is No Distraction

cyber security risk management

Summary: A recent report by the FBI's Internet Crime Center provides stats and examples of some real cybercrime risks out there. We give you the highlights.

Globally, 45% of adult smartphone users say they worry they are too connected to their phones, according to Deloitte. The same percentage says that they try to limit their phone usage in various ways. Of note, some 67% of 18 to 24Y olds say they use their phone too much. It looks like most people worldwide need to work on decreasing their smartphone distractions.

In banking, there is a lot going on well beyond simple distraction when it comes to cybercrime. In fact, a recent report by the FBI's Internet Crime Complaint Center (IC3) provides stats and examples of some real risks out there.

Since its inception, IC3 has handled 1.4mm complaints, representing an average of 800/day and amounting to $5.5B in losses. Those losses have been on the rise for years, increasing from $781mm in 2013 to $1.4B in 2017. Of course, these statistics just represent the amounts tracked by IC3 through its own complaint process. Other studies put cybercrime losses globally at $3T in 2015 with projections of $6T by 2021.

In its report, IC3 indicates the most commonly reported cybercrimes were non-payment and non-delivery, personal data breaches, and phishing/vishing/smishing/pharming scams. Meanwhile, the most common crime types in terms of dollar loss were business/other email compromise (BEC), non-payment/non-delivery, and investment scams.

BEC alone claimed over $676mm in losses or about 3x the amount of the next highest complaint. BEC has morphed into not only asking for wire transfers from fraudulent executive direction, but also scamming wage and tax information and contributing to real estate fraud losses.

Although not as widespread, be aware that tech support fraud saw a 90% increase in losses from 2016 to 2017. Criminals act as tech support to gain access to devices with sensitive information.

These areas of internet risk are most likely covered in your employee cyber training; yet, hearing that these risks are still alive and well may prompt you to refresh that training.

Surely, one of the biggest challenges in combatting cybercrime is staying current on the latest scams. One bold scam highlighted in the report involved impersonated bankers. Criminals based in West Africa posed as executives of BB&T or JPMorgan Chase and contacted potential investors via phone and the internet. Phony domain names were used that were nearly identical to those run by the banks, and the investors received fake documents that had all the appearances of authenticity. They even set up in-person meetings with phony bank representatives. Needless to say, by the time law enforcement cracked the scheme, the bad guys had taken all the money and disappeared.

The good news for community banks is that you know your customers, investors and often even potential customers in the community. So, the chances of this scenario happening are hopefully reduced. Still, it shows

how far many cyber criminals will go to defraud people, so vigilance is critical.

We hope this update can help keep everyone a little safer, while working on some of those smartphone distractions.

CHECK IMAGING FOR CANADIAN CASH LETTERS

PCBB's enhanced cash letter service for Canadian checks can help your bank minimize its credit exposure, increase operational efficiency and deliver faster fraud notification. Learn more about our check imaging for Canadian cash letters.