The Psychology Of Identity Theft

cyber security technology biometrics

Summary: Cyber thieves will typically go after the lowest hanging fruit. Areas of concern for banks: new account application fraud and deposit account hijacking. What can your bank do to mitigate these?

Psychologists now say knowing someone occurs when that person actively shares information with you that is particularly intimate or private. The difference between this sort of knowing someone and knowing about someone is where the line is drawn. Knowing about someone occurs when you may not even know the person, but you know things about them that make you feel like you might know them, if you met them. The example most often given here is that of a celebrity, where you may know a lot about him/her, but you have never met.

Knowing someone and possessing knowledge are very important in banking too. After all, common knowledge shows community banks know their customers way better than the biggest banks.

A question that surfaces here is how to know your customer when they are also using hundreds of digital channels as well as physical ones. People interact more and more through both large and small screens, so knowing someone becomes more difficult in one way because that human to human contact piece that is so critical to the strongest relationships has eroded over time.

Making matters worse, there are also many bad actors floating around the banking space, stealing identities and then using those fake credentials to wreak financial havoc.

Identity theft is nothing new. Long before there even was a mainstream internet, crooks were stealing personal information in order to take over legitimate customer accounts, or create fake accounts for the purposes of defrauding a company. Today, the online world gives cybercriminals even more fertile ground. They can not only research and more easily reach victims, but can also more readily peddle stolen data on the dark web.

One truism of criminal activity is that thieves will typically go after the lowest hanging fruit. One such area is in new account application fraud. Here, crooks use a real person's information, or a "synthetic identity" created from legitimate information from several people, to open a new loan account and then drain it before the bank catches on to the fact that the borrower is not who they claim to be. Application fraud in particular has been on the rise, according to research firms like Aite Group and Javelin Strategy & Research, so banks should be wary.

Meanwhile, the FDIC warns banks that deposit account hijacking is also an issue. While there are a limited number of ways to hijack deposit accounts, each one leverages stolen information. Here, the most common methods are through phishing, hacking, retrieving hard-copy documents, looking over someone's shoulder, using insiders and loading malicious software onto a computer used by consumers.

In the battle against the identity-stealing bad guys, all banks are under pressure. While there is no magic bullet to correct the growing problem of identity theft, you may find these steps helpful as you seek to mitigate its incidence and impact:

Educate customers. Even today there are still huge holes in how people protect their identity. An Experian survey finds 43% of people shop online using a public Wi-Fi connection, 25% have shared their credit card

number or PIN with friends and 20% say they would allow someone to use their personal information to get a job or line of credit. Clearly more education is needed, so keep informing customers about the very real threat of identity theft and all the difficulties it can cause.

Practice engagement. The same Experian survey shockingly finds 53% of people don't worry about identify theft at all because they say banks and credit card companies monitor their accounts. As a result, almost half (48%) say they don't bother to regularly check their credit report for errors or suspicious activity. Staying actively engaged in one's financial wellbeing is critical for customers and employees, so tell everyone.

Alert your customers. If your bank offers it, be sure to provide alerts to customers. It can help them protect their information and identity, as they proactively monitor suspicious activity.

Remind your customers. Be sure to continually remind customers you do not and will not ask for sensitive information by email. Share information about scams targeting bank customers provided by professionals and regulators. One such example is from the FDIC called "10 Scams Targeting Bank Customers".

Knowing someone these days is in some ways easier and in some ways more difficult so we hope this helps your team.

INTRODUCING 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.