Authenticating The Two-Factor Text

cyber security technology risk management

Summary: Many banks use text message authentication, but thieves are finding ways to hack it. We provide an update along with tips to keep you and your customers safe.

Statista research finds the percentage of the US population with a social media profile is running at about 77% right now. Even more interesting perhaps is that it declined from 80%, as of the end of 2017. Maybe we aren't as social as we once were or maybe this is a result of the largest social media platforms deleting accounts they are unable to authenticate.

Speaking of authentication, in banking, we note that many banks no longer rely solely on passwords anymore. Today, banks rely more on two factor authentication (2FA). This type of authentication checks a user's identity using a combination of two different pieces of evidence (factors) such as, something the user knows, and either something the user has, or something the user is. A typical example here is a logon ID with a password and a system generated code sent to the user's mobile phone or email.

The problem is that as with most things, the bad guys are pretty good at breaking nearly any security protocol. Since many banks use text messages as the second factor, this is worth reviewing.

These days, hackers can more easily bypass weak 2FA implementations. They do this by either intercepting software codes or exploiting account-recovery systems. Some hackers have even targeted phone carriers to get to bank account information by rerouting and forwarding codes in transit, to their evil lairs. Bankers should be careful here and when something seems the least bit odd with a customer- ask, ask, and ask again.

Another way thieves acquire texted authentication codes can be to send an unsuspecting person a text or to simply call their mobile number. Thieves then pose as a bank representative and claim they have seen suspicious account activity. The scammer then makes a big to-do about not giving them any personal information for security reasons, but tells the customer to expect a text from the bank asking for an authorization code to fix the problem. The thief then attempts to log into the customer's online account using previously stolen login information and when the actual text message code is sent to the customer for authorization, he provides it to the thief, thinking it's the bank.

These examples show the downside to using phone numbers as proof of identity, yet there are efforts afoot to shore up security. Four major US wireless carriers have teamed up on "Project Verify", an app due out next year that is supposed to seamlessly verify the user's identity using a multi-factor profile based on their personal mobile device. While this doesn't do much good if the user's phone is stolen, it is a big step in the right direction.

In the meantime, banks must continue to take a multi-pronged approach to security and authentication. This includes things such as passwords, 2FA and even biometrics perhaps. Of course, you can also employ passive authentication. This is where technology is used to detect whether a SIM card is the same one that has been used for past transactions, and where the signal is coming from, to try to detect geographic location anomalies.

While nothing is foolproof, when multiple types of security barriers are erected, it's harder for thieves to break through. We know you are working hard to stay vigilant, and we will continue to provide you with helpful updates along the way no matter the social media or other platforms your customers are using.

ON DEMAND HELP FOR COMMUNITY BANKERS

Community bankers face many difficult challenges every year, but you are not alone. Our experts stand ready to help you address a variety of issues. Go here to view options and opportunities.