How To Mitigate Rising Mobile Fraud

mobile banking fraud protection phishing

Summary: It is not surprising that mobile fraud is surging, as the US has over 294MM smartphone users. Community financial institutions need to stay aware, meticulously authenticate customers' identities, and communicate the latest scams to their customers to stay out of harm's way. Here are three of the latest mobile phone scams and how to stay out of trouble.

Did you know that the medical term for goosebumps is cutis anserine? Taken directly, this means goose skin and is when the hair follicles rise up due to flexing of the skin. It often results from an involuntary reaction of fight or flight. In animals, this reaction helps them appear more puffed up and bigger as a dangerous adversary. While the value to humans is less obvious, many of us may get goosebumps when we hear about the latest mobile scams.

The US has over 294MM smartphone users and hit an 85% penetration rate in February 2021. So, it is not so surprising that mobile phone scams are on the rise. More than half of Americans last year got a scam call or a text message, and mobile phones are now the hot ticket for fraudsters over landlines, according to Truecaller. Overall, 60MM people were tricked, for an average loss of $502 and a collective loss of about $30B.

With this growing area of fraud, CFIs need to stay up-to-date and educate their customers to mitigate any damage. Here are some of the **latest mobile phone scams and how to steer clear**.

1. **"Smishing," or phishing by text.** "*Threat actors are purchasing lists of mobile phone numbers and trying all types of schemes,*" says one IT consultant. "*Many are suggesting you have a payment due, or thank you for your payment, or click here to complete a survey. In each case the threat actor wants you to click a link where they'll either ask for your user credentials or attempt to install malicious coding on a mobile device.*" Fraudsters can then use credentials to obtain one-time authorization codes sent via SMS for entrance into the user's various accounts.

Luckily, many people realize the danger with these texts. According to Truecaller, 65% of those surveyed reported that they would delete a text from a number they did not recognize. Still, it never hurts to **remind your customers that they shouldn't click any unsolicited links** on their mobile phone, the same protocol as an email with links. If they think the request may be valid, they should contact the organization directly first.

2. **Automated threats.** The FBI uncovered an "evil emulator farm" — a fraud group employing 20 emulators, or virtual mobile devices, that mimicked 16K real devices. Through manipulated automation, the emulators were able to impersonate the real users' interactions with their devices to receive one-time codes to complete fraudulent transactions worth millions.

To circumvent both smishing and automated threats, CFIs should **send one-time codes through the institution's mobile app** and not through texts. Make sure to register both the customer's phone number and actual device, as this is something fraudsters can't get to virtually. Upon activation, CFIs then send push notifications through encrypted channels, tying a customer's device to the app. Once devices are registered to a CFI's app, their hardware security features also make it tougher for fraudsters to steal identifiers. With

multiple security layers, **biometric authentication confirmed by push notification** stops fraudsters with stolen biometrics from virtually impersonating customers.

While it is always best to maximize security, there are ways to mitigate this fraud, while minimizing the disruption to the customer experience: **zero-factor authentication** (0FA) and **app shielding**. Some institutions are now employing 0FA, which uses network, location, and device signals to recognize users seamlessly, using sensors and mobile technologies. This is done behind the scenes, so minimal customer effort is needed. App shielding can also be deployed, which shuts down banking apps, if malicious threats are detected. According to Information Age, "*App shielding ensures strong security against unknown threats on untrusted devices, but the security mechanisms they rely on have little to no impact on the user experience.*"

3. **Live-calling social engineering scams.** Oftentimes, the caller is looking for a lonely, vulnerable, or naïve person. They may even be nice and helpful. Or they could be threatening and mean. There are many varieties of these types of scams, including:

- Impersonating the Social Security Administration or the IRS
- Debt relief and credit repair
- Business coaching
- Investment opportunities
- "Free" trials that then bill monthly
- Prize and lottery

A recent kidnapping scam showed how far these scammers will go. The bad guy called a victim at home in the early morning, using "phone masking technology on a voice over IP internet phone" that indicated he was using a relative's phone. "*He said that he had kidnapped the relative – with a woman crying in the background, and demanded that he pay the kidnappers $1,000 or they would kill them.*"

The low amount prompted the victim not to hesitate to send payment to an anonymous Venmo account. Fortunately, Venmo stopped the transaction because of earlier notices about this scam. CFIs should educate their customers not only to question strange situations such as this, but also to tie their insured checking account or credit card account to Venmo, so they can always be reimbursed.

CFIs should **educate their customers to disregard fake caller IDs, hang up, and consider call blocking** Still, this won't stop them from trying again, so being on constant guard is key.

It is not easy to stay on top of all the latest scams. But, staying informed, diligently authenticating, and keeping your customers educated will mitigate the damage. Keep your guard up!

YOUR INTERNATIONAL PLATFORM OR OURS? YOU CHOOSE!

Your team can automatically send international wires using your own existing domestic platform, or our proprietary platform. Learn more by contacting us today.

ECONOMY & RATES

Rates As Of: 03/07/2022 04:23PM (GMT-0700)

Treasury	Yields	MTD Chg	YTD Chg
3M	0.38	0.03	0.32
6M	0.75	0.06	0.56

1Y	1.06	0.06	0.67
2Y	1.56	0.12	0.82
5Y	1.71	-0.01	0.44
10Y	1.78	-0.05	0.26
30Y	2.19	0.02	0.28

FF Market	**FF Disc**	**IORB**
0.08	0.25	0.15

SOFR	**Prime**	**OBFR**
0.05	3.25	0.07