New scam aims to trick you into giving up your cell phone account information

3 April 2019, by Eli Blumenthal, USA Today

If someone calls you pretending to be from your cell phone carrier and asks for a verification code, don't give it to them.

That was a lesson learned in Florida last month after two different scammers tried to buy phones at a Clearwater, Florida, Verizon store.

The two scammers, Ah'jhzae Diamondric Artag Berry and Keith Ramsey, had apparently tricked two unsuspecting victims in an attempt to purchase new devices on the victims' accounts.

Both scammers were busted at the store after Verizon alerted local police to the irregularity. Clearwater police department tells USA TODAY that the victims were unrelated, however, the department is not sure if there is a link between the two cases.

Ramsey was trying to buy two iPhone XS Max phones valued at $1,200 per device on March 26. Berry was trying to purchase a single phone that was valued at $1,250 or March 21, police told USA Today.

Tim Downes, detective sergeant for the department's economic crimes unit, says Ramsey's scheme started with getting the victim's email address and sending his target a false message impersonating Verizon saying that there was fraud on the account with a number to contact. "That's a bad number, so basically if you respond to that email you are going to get the bad guy," Downes says.

If you call back, the fraudster says they will send you a personal identification number, or PIN code, that they will want you to tell them. By giving them the PIN over the phone the scammer exploits the password reset verification system that Verizon has put in place to confirm that you are you.

Once they have that PIN, they can reset the password, make themselves a "master account user" on your account and otherwise do what they want, including forwarding calls or going into a store and buying devices as that primary user.

They'd have to pay taxes and some fees in the store on a new device purchase but could otherwise leave you footing the majority of the bill while they sell the device for a profit.

Luckily, in this case, the Verizon store noticed how quickly the account changed and notified the police allowing both suspects to be apprehended while they were in the store.

"We recognize that the privacy and security of information is of paramount importance to our customers. Unfortunately, it's a harsh reality that bad actors are always looking for ways to engage in fraud and identity theft," Verizon spokesperson Steve Van Dinter said in a statement provided to USA TODAY.

"As fraudsters gather more private information from the dark web and create more authentic looking fake identification, our teams at Verizon are always working to stop these criminals who impact about 7,000 customers every month."

If you suspect fraud, Verizon recommends contacting them directly at (800) 922-0204.

While cell phone fraud has been going on for years, Downes says that this method, exploiting the security measures against the victim, is new.

So how can you protect yourself? He recommends checking the companies you deal with and being aware of the ways they interact with you. Verizon, for example, would never ask for those identification PINs they text you to confirm your identity.

When in doubt, you can and should reach out to the
company directly instead of responding to "them" reaching out to you.

"People are getting smarter and more sophisticated, and it's going to be more difficult to prevent these things from happening," in the future, Downes says.

"Be careful with these emails that you get, and people should be monitoring all their accounts and their credit report just to make sure everything is the way it should be," he adds.

"That goes a long way in helping to stop and prevent these frauds from happening."

(c)2019 USA Today
Distributed by Tribune Content Agency, LLC.

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.