TECH JUN 27 2016, 1:46 PM ET

Fraud Alert: ID Thieves Hijack Mobile Phone Accounts

by HERB WEISBAUM

Identity thieves have come up with another devious way to make money by pretending to be someone else — hijacking mobile phone accounts.

While a common criminal might try to snatch your smartphone for some quick cash, these clever crooks take over your wireless account.

“Mobile accounts are now a prime target for identity thieves,” said Eva Velasquez, president and CEO of the non-profit Identity Theft Resource Center. “It’s probably one of the easiest forms of identity theft to commit and it’s very lucrative.”

By taking control of your mobile account, a fraudster can buy new equipment, such as expensive smartphones, bill them to your account and then sell them.

Read More: Feds Propose New Payday Loan Rules to End 'Debt Trap'

“This type of fraud is a form of money laundering,” said Robert Siciliano, CEO of IDTheftSecurity.com. “They’re turning someone’s personal information into cash by buying the phones and then selling them.”

Dena Haritos Tsamitis had her mobile account hijacked in March.

After she suddenly lost service, Tsamitis contacted her mobile carrier. They said she had gone to a store in New York City and upgraded two of her phones to iPhones and then shut down her old devices. Tsamitis lives in Pittsburgh and had not been to New York and had not authorized any changes to her account.

To restore her service, Tsamitis had to go to her carrier’s local store, present ID and get new SIM cards.

“It was a nightmare. It was hugely inconvenient and caused a lot of stress, but it would have been much worse had I needed to use the phone,” she said. “I had to cancel all of my meetings and spend the next day in the phone store.”

Tsamitis, who teaches cybersecurity at Carnegie Mellon University, told NBC News she knows her account was not hacked. It was hijacked by an identity thief who went to the store in person.

Wireless carriers are aware of the problem and tell NBC News they are working to prevent it.

“We see this as another example of the evolving landscape of identity theft,” said Jacqueline McCarthy, director of regulatory affairs at CTIA-The Wireless Association.

“Our carriers have a variety of procedures in place — these include verifying passwords and other credentials — to authenticate transactions when their subscribers seek to activate a new mobile device or make changes to their service.”

CTIA says wireless carriers are also training customer service representatives about the fraud and how to spot it. The mobile phone companies are also working with law enforcement to investigate these crimes. The association has consumer security and privacy tips on its website.

A growing problem most customers don’t know about

Lorrie Cranor had her phone number hijacked a few weeks ago, though she didn’t realize what was happening at the time. It just seemed like some sort of glitch caused her smartphone and her husband’s to both go dead on the same day.

When she called her carrier, the customer service representative wanted to know if the problem was with her new iPhone. Cranor didn’t have a new iPhone.

“We found out that someone had gone into the phone store in another city with a fake ID and said they wanted to upgrade their phones,” Cranor said. “They walked out with two brand new iPhones with our phone numbers on them and charged to our account.”

Cranor, who happens to be the chief technologist for the Federal Trade Commission (FTC), decided to investigate the crime and recently wrote a detailed warning about it.

“We’ve been getting complaints about this for several years, but the number and frequency of the complaints is definitely going up recently,” Cranor told NBC News.

Read More: Glitters, but Not Gold: Fake Gold and Silver Coins 'Flooding' Market

The FTC’s complaint database shows that in January of 2013 the agency received 1,038 incidents of mobile account hijacking. This past January, the number had more than doubled to 2,658. Cranor found that all four of the major carriers are experiencing this problem. It’s more than an inconvenience

Imagine how frustrating it would be to find that your mobile device suddenly lost service — especially if you’re on a business trip or away on vacation.

If the crook simply gets new phones and sells them, there’s no financial harm to you. The wireless phone company takes the loss for that stolen equipment.

But if the ID thief keeps the phone, the potential harm is much greater.

Many of us now have accounts that require two-factor authentication (2FA) — where a unique code is sent to our mobile device. It’s becoming an increasingly important way to verify someone’s identity online when they try to log onto financial and social media accounts.

This added security is based on the assumption that someone who steals your password doesn't also have your phone. But 2FA breaks down when a crook has your phone number and gets those verification codes.

"Taking over someone's phone account means you can also take over their bank account," said Rodger Desai, CEO and co-founder of Payfone, a company that works with banks and mobile carriers to spot such fraud. "It's becoming a more common occurrence that's happening even more because it's such an easy way to break into phone company accounts."

Until you realize there's a problem and have those hijacked phones turned off, the criminals can also load mobile payment services onto the phone and go shopping.

"I buy that stolen credit card number for 25 cents or so on the dark web, and I simply type that into Apple Pay," Desai explained. "I know the only check the bank is going to do is send you this one-time passcode. If I've taken over your phone account, then I get that passcode and now I can shop very securely with your money."

As chip-enabled credit cards make it harder to create counterfeit cards with stolen account numbers, crooks will look for other ways to monetize this information.

More could be done

Debbie Matties, vice president of privacy at CTIA, says the industry is working "very diligently" to combat this fraud. Because the mobile phone companies take the loss on this stolen equipment, "they have a very strong interest in curtailing the problem," she said.

Security experts contacted by NBC News want to see mobile phone companies do more to protect their customers by improving their authentication techniques.

“The fact that organized crime is now engaged in this scam means that the carriers need to beef up their authentication processes and procedures so that no one can just walk into an authorized dealer and take over your account,” said IDTheftSecurity.com’s Robert Siciliano.

Read More: Should You 'Freeze' Your Credit Files to Lock Out ID Thieves?

The FTC’s Lorrie Cranor believes more could and should be done. She says the carriers rely too heavily on photo ID.

“It’s just too easy to provide a fake driver’s license and it’s not clear that all the store employees are trained on how to detect that,” she said.

Cranor would like to the carriers adopt “a multi-level approach to authenticating both existing and new customers” and require their employees as well as third-party retailers to use it for all transactions.

There is something you can do to protect yourself — create a password or PIN that’s required before any changes can be made to your mobile account.

Cranor found that each of the four major carriers — AT&T, T-Mobile, Sprint and Verizon — offers this feature in a slightly different way. In her blog post, "Your mobile phone account could be hijacked by an identity thief," she gives the specifics for each company.

Herb Weisbaum is The ConsumerMan. Follow him on Facebook and Twitter or visit The ConsumerMan website.
