What's worse than thieves hacking into your bank account? When they steal your phone number, too

July 14 2024, by Fatima Hussein

A person uses a cell phone on Saturday, July 13, 2024, in Los Angeles. The FBI Internet Crime Complaint Center reports that SIM-swapping complaints have increased more than 400% from 2018 to 2021. New federal regulations aimed at preventing port-out hijacking are under review, but it's not clear how far they will go in stopping the crime. When your own phone access is lost to a criminal, the very steps you once took to protect your accounts — such as two-factor

authentication — can be used against you. Credit: AP Photo/Paula Ulichney

One Monday morning in May, I woke up and grabbed my cell phone to read the news and scroll through memes. But it was out of cell service. I couldn't make calls or texts.

That, though, turned out to be the least of my problems.

Using my home Wi-Fi connection, I checked my email and discovered a notification that $20,000 was being transferred from my credit card to an unfamiliar Discover Bank account.

I thwarted that transfer and reported the cell phone issues, but my nightmare was just starting. Days later, someone managed to transfer $19,000 from my credit card to the same strange bank account.

I was the victim of a type of fraud known as port-out hijacking, also called SIM-swapping. It's a less-common form of identity theft. New federal regulations aimed at preventing port-out hijacking are under review, but it's not clear how far they will go in stopping the crime.

Port-out hijacking goes a step beyond hacking into a store, bank or credit card account. In this case, the thieves take over your phone number. Any calls or texts go to them, not to you.

When your own phone access is lost to a criminal, the very steps you once took to protect your accounts, such as two-factor authentication, can be used against you. It doesn't help to have a bank send a text to verify a transaction when the phone receiving the text is in the hands of the very person trying to break into your account.

Even if you're a relatively tech-savvy individual who follows every recommendation on how to protect your tech and identity, it can still happen to you.

Experts say these scams will only increase and become more sophisticated, and the data show they are on the rise.

I am not the most tech savvy person, but I am a law-school educated journalist who specializes in finance reporting. Due to the very online nature of my job, I was taught all the methods of staying safe online: constantly changing my passwords with multi-factor authentication, signing out of apps that I don't use regularly and keeping my personal information off the internet.

Still, despite being safe, I was vulnerable to criminals. And it took a lot of time and legwork before I got my money and phone number back.

The FBI Internet Crime Complaint Center reports SIM-swapping complaints have increased more than 400% from 2018 to 2021, having received 1,611 SIM swapping complaints with personal losses of more than $68 million.

Complaints to the FCC about the crime have doubled, from 275 complaints in 2020 to 550 reports in 2023.

Rachel Tobac, CEO of SocialProof Security, an online security company, says the rate of the crime is likely much higher since most identity thefts are not reported.

She also says two-factor authentication is an outdated way of keeping consumers safe, since it's possible to find anyone's phone number, birthday and social security number through any number of public or private databases on the web.

The ability of thieves to obtain your personal information was again made clear Friday when AT&T said the data of nearly all of its customers was downloaded to a third-party platform in a security breach two years ago. Although AT&T claims no personal information was leaked, cybersecurity experts have warned breaches involving telephone companies leave customers vulnerable to SIM swapping.

As of now, switching numbers from one phone to another is easy and can be done online or over the phone. The process takes less than a few hours so long as a criminal has your personal information on hand.

While consumers need to be smart about having a variety of different passwords and protections, consumers need to "put pressure on companies where its their job to protect our data," Tobac said.

"We need them to update consumer protection protocols," she said, since two-factor authentication is not enough.

FCC rules have recently changed to force companies to do more to protect consumers from this type of scam.

In 2023, the FCC introduced rulemaking that require wireless providers to "adopt secure methods of authenticating a customer before redirecting a customer's phone number to a new device or provider" among other new rules. Companies could require more information when a customer tries to port over a phone number to another phone—from requiring government identification, voice verification or additional security questions.

The rules were scheduled to take effect on July 8, but the FCC on July 5 granted phone companies a waiver that delays implementation until the White House Office of Management conducts a further review.

The wireless industry had sought the delay, stating among other reasons that companies need more time to comply. CTIA, which lobbies on behalf of the companies, said the new rules will require major changes in technology and procedures both within the wireless companies and in their interactions with phone manufacturers.

But if the FCC rules had been in place, my phone number might have been harder to steal, experts say.

Ohio State University Professor Amy Schmitz says the new FCC rules make it easier for consumers to protect themselves, but it is still reliant on action and awareness of the consumers.

"I still question whether consumers will be aware of this, and will take action to protect themselves," she said.

It took ten days to get my number back from Cricket Wireless—and that wasn't until I told company representatives that I was writing a story about my experience.

In that period of time the scammer was able to access my bank account three times and eventually successfully transferred $19,000 from my credit card— even though I removed my number from the bank account, froze my credit, changed all my passwords, among other measures.

Bank of America worked to reverse the $19,000 wire after I visited a branch near the AP bureau in Washington.

Cricket apologized for the error and said in an email that its "expectation is to deliver a much better customer experience."

"Fraudulent port-outs are a form of theft committed by sophisticated criminals," reads a company statement that was emailed to me. "We have

measures in place to help defeat them, and we work closely with law enforcement, our industry and consumers to help prevent this type of crime."

An AT&T representative told me in an email that "all providers are working to implement the FCC's new rules on port-outs and SIM swaps."

I'm still unsure of how this person got access to my accounts, whether through my social security number, phone number or date of birth, or possibly a recording of my voice.

It was a hard lesson in how vulnerable we are when you lose control of our personal information that is so publicly available.

Citation: What's worse than thieves hacking into your bank account? When they steal your phone number, too (2024, July 14) retrieved 10 September 2024 from https://techxplore.com/news/2024-07-worse-thieves-hacking-bank-account.html