# Liz Weston: In 'SIM swap,' criminals really have your number

14 October 2019, by Liz Weston Of Nerdwallet

This April 2017, file photo provided by NerdWallet shows Liz Weston, a columnist for personal finance website NerdWallet.com. (NerdWallet via AP, File)

If you're not familiar with SIM swap fraud, prepare to be terrified.

This scam, also known as port-out or SIM splitting fraud, allows criminals to hijack your cell phone number. Once they have your number, the bad guys can clean out your financial accounts, confiscate your email, delete your data and take over your social media profiles.

Fraudsters can do all this because many companies—including banks, brokerages, email providers and social media platforms—verify your identity by texting a code to your cell phone. Intercepting those codes can give a criminal an all-access pass to your financial and digital life.

This kind of identify fraud has been around for years, but it's getting more attention after a wave of cryptocurrency thefts and attacks on high profile victims, including Twitter CEO Jack Dors ey, who briefly lost control of his Twitter account.

THIS IS THE FRAUD THE EXPERTS FEAR MOST

The potential damage is so great that security expert Avivah Litan, vice president at research firm Gartner Inc., fears losing her phone number far more than having her Social Security number compromised.

"I'd rather they took my social, to tell you the truth," Litan says, "because I care about my retirement money and I know some of it's protected through phone number access."

What's more, you can't prevent this fraud—only your carrier can. And right now, criminals are finding it's pretty easy to fool the phone companies.

Sometimes the scam artists bribe or blackmail carrier employees; sometimes, the employees are the criminals. Other times, the fraudsters use identifying data they've stolen, bought on the dark web or gleaned from social media to convince carriers that they're you. They pretend they want to change carriers or say they need a new SIM card, the module that identifies a phone's owner and allows it to connect to a network. Once they persuade the carrier to transfer your number to a phone they control, they can attack your other accounts.

Even getting your cell phone carrier to recognize what's happening, and help you stop it, can be a challenge, says security expert Bob Sullivan, host of the "So, Bob" technology podcast. Victims report being forced to educate phone company employees about the fraud and having their numbers stolen more than once, even after protections were supposedly in place.

"The real problem is when you call, are you going to get a person that you can talk to about this

quickly and are they going to recognize what's happening?" Sullivan asks. "Or are you going to be in voicemail hell for three hours while a criminal raids all your accounts?"

Phone companies protest they're doing all they can, and solutions that would make this theft harder also would inconvenience people who legitimately want to switch carriers or need their numbers transferred to new SIM cards because their phones have been lost or stolen.

While you can't prevent this fraud if you have a cell phone, you may be able to reduce the chances of being victimized or at least limit the damage.

CHANGE HOW YOU'RE IDENTIFIED, IF YOU CAN

First, ask your phone company to put a personal identification number on your account. Hopefully the carrier will require that to be produced before your phone number is "ported out" to a new carrier or assigned to a different SIM card.

Then, investigate whether you can switch to more secure authentication on your sensitive accounts. Being texted a code is better than nothing, since this "two factor" authentication is harder to beat than just using a password. Better options would be to get the codes through a call to a landline or by using an authenticator app such as Authy, Google Authenticator or Duo Security on your smartphone.

ASSUME THE WORST

If your phone stops working or you can't send or receive texts, don't assume it's a glitch. Call using an alternate method or visit your carrier immediately to report phone takeover fraud. Sullivan recommends knowing a few alternate ways to contact your carrier, such as Wi-Fi calling, Skype or an easily accessed backup phone.

If you do become a victim, you should:

— Alert your financial institutions.

— Change the email and password associated with all your financial and payment accounts.

— Freeze your credit reports.

— File identity theft reports with your local police department.

The important thing is to move quickly, because the bad guys won't wait.

"You have a plan in place because minutes are going to matter," Sullivan says.