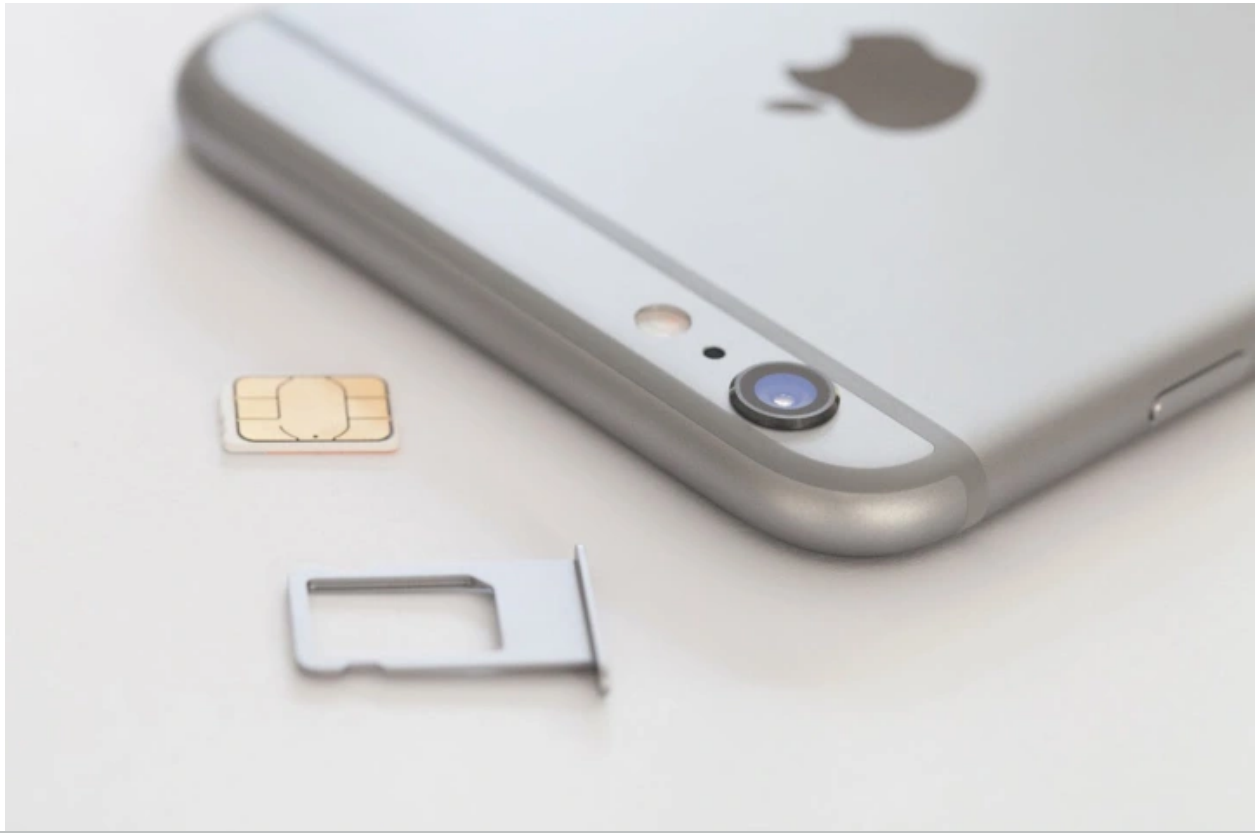
Here's how to stop SIM fraudsters from draining your bank account

By Kyle Wiggers
July 6, 2017



sophisticated form of fraud that allows hackers to gain access to bank accounts, credit card numbers, and other personal data. It's tough to spot, and even tougher to undo the resulting damage.

It's a growing trend. According to the U.S. Fair Trade Commission, there were 1,038 reported incidents of SIM swap identity theft in January 2013, representing 3.2 percent of identity theft cases that month. By January 2016, that number had ballooned to 2,658.

But there's hope. Knowing SIM card fraud's basics can help protect you against the most common forms, and recognizing an attack in progress can help you head off the worst of its effects.

What is a SIM swap scam?

A cellphone SIM card stores user data in GSM (Global System for Mobile) phones. They're principally used to authenticate cellphone subscriptions — without a SIM card, GSM phones aren't able to tap into any mobile network.

SIM swap fraud is a type of identity theft that exploits the SIM system's biggest vulnerability: Platform agnosticism.

"Unlike mobile malware, SIM fraud attacks are usually aimed at profitable victims that have been specifically targeted through social engineering."

"It's a way attackers are attempting to gain access to their target's cell phone communications," Andrew Blaich, a security researcher at Lookout, told Digital Trends. "There are many public cases of attackers social engineering their way through a cellular company's representative to get a SIM card issued for an account the attacker doesn't own or have access to. It appears to be easy to do as all you need is a willing/susceptible representative at any cellular phone store."

Emma Mohan-Satta, a fraud prevention consultant at Kaspersky Labs, told Digital Trends that a growing reliance on phone-based authentication has made SIM swapping an increasingly lucrative enterprise.

"A high proportion of banking customers now have mobile phone numbers linked with their accounts, and so this attack is becoming common in some regions where this attack was not previously so common," Mohan-Satta said. "Unlike mobile malware, SIM fraud attacks are usually aimed at profitable victims that have been specifically targeted through successful social engineering."

Laying the groundwork for a SIM swap scheme involves collecting as much information about the victim as possible. Fraudsters might send phishing mail — messages that impersonate legitimate businesses like credit card companies and health insurers — intended to fool victims into forking over their legal names, dates of birth, addresses, and phone numbers. Unfortunately, many people can't tell the difference between real emails and phishing emails. Alternatively, they might scrape public websites, social media, and data dumps from criminals who specialize in collecting personal data.

Once SIM criminals have gathered enough information on a target, they create a false identity. First, they call the victim's cellphone provider and claim that his or her SIM card has been lost or damaged. Then, they ask the customer service representative activate a SIM card or number in their possession.

Most cellphone service providers won't acquiesce to those requests unless callers answers security questions, but SIM fraudsters come prepared, using the personal data they've collected from across the web to defeat the carrier's security checks without raising any alarms.

Once they've gained unfettered access to a victim's phone number, criminals target bank accounts.

"The attacker can read your SMS messages and see who you're chatting with and what about," Blaich said. "Many banks will send you a code to log into an account or reset a password to a mobile phone via SMS, which means an attacker committing SIM fraud can request and receive the code and access your bank."

transfer between the two accounts, it appears to the bank's computer system as though the victim is transferring funds between two parallel accounts.

Signs of SIM swap fraud

It's tough to detect SIM card fraud before it happens. Most victims discover they've been compromised when they try to place a call or text. Once the perpetrators deactivate a SIM, messages and calls won't go through. But some banks and carriers have instituted protections that prevent SIM swap fraud before it happens.

"There are multiple organizational and technical ways to combat SIM fraud — from introducing user alerting and additional checks for SIM reissuing to sharing knowledge of SIM swap activity between banks and phone companies," Mohan-Satta said. "Banks can also consider looking for behavioral changes through behavioral analysis technology that can indicate a compromised device. This information may then be used by a bank to avoid sending SMS passwords to compromised devices and as an early way to alert the genuine customer."

Some institutions call customers to determine whether they got a new SIM card or alert them that someone is potentially impersonating them.

Martin Warwick, FICO's fraud chief in Europe, the Middle East, and Africa, told CreditCards.com that an increasing number of banks use the IMSI (International Mobile Subscriber Identity) — a unique number associated with a specific GSM phone — to ensure one-time use codes are sent only to legitimate subscribers.

"It is possible to check whether your SIM card number and your international mobile subscriber identity (IMSI) are the same," Warwick said. "If there is a discrepancy, your bank could contact you by email or landline to check."

Banks in the U.K., including the Lloyds Banking Group and Santander, say they're working with network providers on the issue. Groups like the Financial Fraud Action UK actively partner with telecommunications companies to educate subscribers about SIM swapping.

How to prevent SIM swap fraud

Major carriers in the U.S. offer security that can help protect against SIM card swapping.

AT&T has "extra security," a feature that requires you provide a passcode for any online or phone interactions with an AT&T customer representative. You can turn it on by logging into AT&T's web dashboard or the myAT&T app.

Sprint asks customers to set a PIN and security questions when they establish service.

T-Mobile lets subscribers create a "care password," which it'll require when they contact T-Mobile customer service by phone. You can set one up by visiting a T-Mobile store or by calling customer care.

Verizon allows customers to set an account PIN, which they can do by editing their profile in their online account, calling customer service, or visiting a Verizon store.

"Users should avoid revealing too much personal data online, and check on what alerts can be set up with their bank or phone company to identify any attempts to access their account," she said.

> *"Avoid using SMS as a primary method of communication because the data is not encrypted."*

Another good practice is using encrypted messaging apps that aren't as prone to snooping as SMS. Blaich suggests enabling two-factor authentication, which requires a randomly generated passcode in addition to a username and password, on sensitive social media, credit card, and bank accounts.

"Users can best protect themselves by using services that don't use SMS for their codes and use authenticator apps like Google Authenticator or any number of other apps that provide a similar service," he said. "You should also avoid using SMS as a primary method of communication because the data in an SMS is not encrypted and is capable of being snooped on easily. Users should switch to messaging apps or services like iMessage, WhatsApp, Signal, etc. for any messages you wish to be private."

It never hurts to exercise due diligence. Blaich recommends checking with your cellphone company every couple of weeks to see if any SIM cards have been issued without your knowledge.

If you're the victim of a SIM swap scam, it's not the end of the world. Mohan-Satta says that acting quickly can minimize the amount of damage inflicted by fraudsters.

"Inform the bank or phone company as soon as you have any suspicions to reduce the impact of the attack," she said.