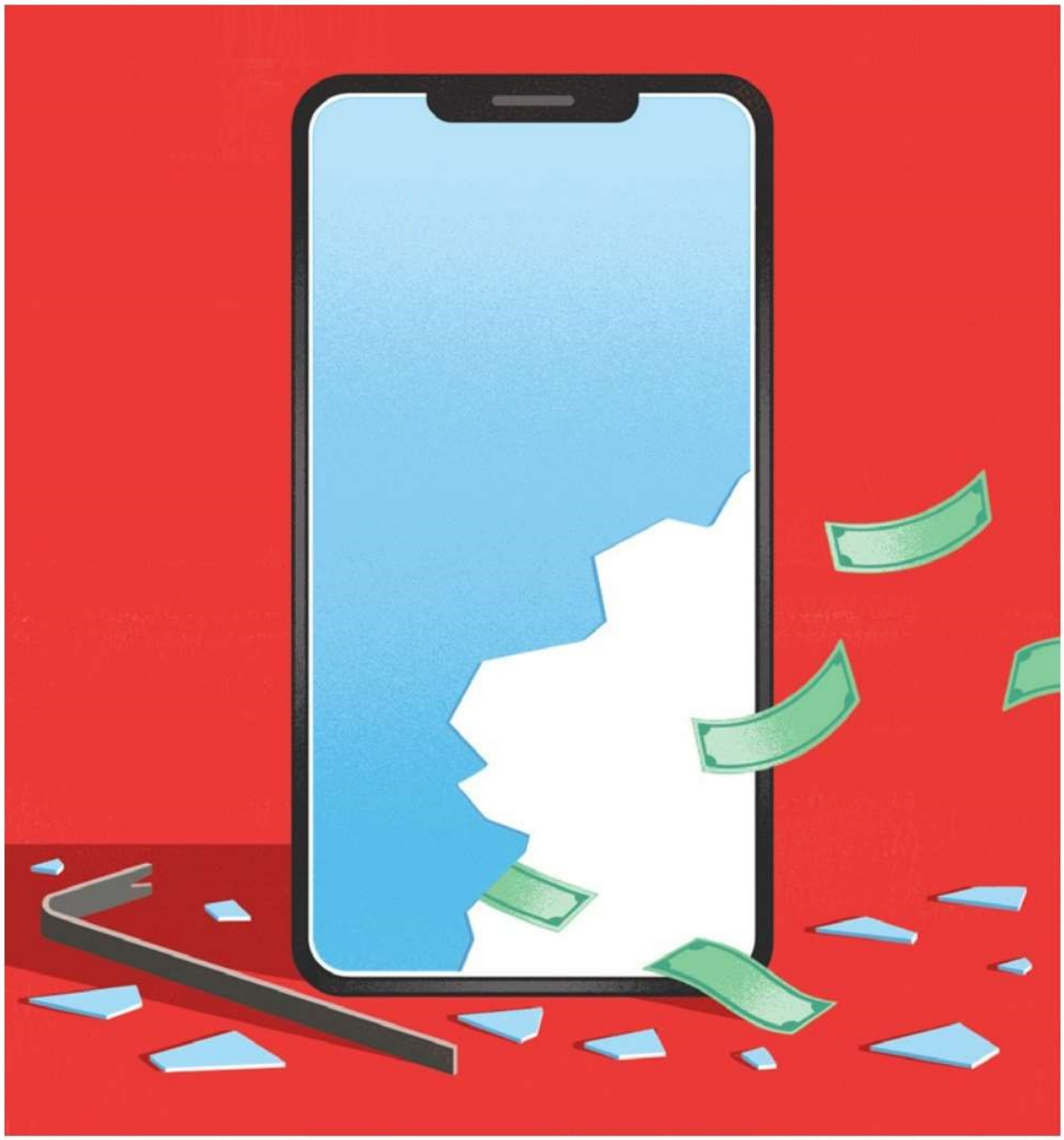
MY PHONE WAS CLONED!

Criminals take over your phone, then drain your bank account. Here's how to prevent it

BY SARI HARRAR



After a relaxing family vacation in Mexico with his wife and their two young sons, Bob Davis switched his phone out of airplane mode as their plane reached the gate of an airport in the Northwestern U.S. last summer. "My phone wasn't connecting to cell service," he says. "I turned it off and back on, but nothing."

Back home, Bob and Jennifer (not their real names to protect their identity) went online and discovered criminals had locked them out of their financial accounts and launched a stealing spree. Scammers ordered an Airbnb gift card, apparently as a wedding present, and bought thousands of dollars of stereo equipment through the family's Amazon account. Worse, the crooks were in the process of transferring $30,000 out of the couple's Coinbase cryptocurrency account. "The thieves had set up an international bank account to try to withdraw the money, but we contacted the company in time to stop it," Jennifer says. "We caught it just in time."

Bob and Jennifer stayed up till 3 a.m., dialing customer service departments for every important financial account, trying to stop the looting. The scammers had changed logins and passwords, so the couple had to prove they were the real owners. In the days that followed, they found out what had happened: They were targets of SIM swapping, a sophisticated cellphone cloning scam that has cost Americans hundreds of millions of dollars.

How it works: Fraudsters start by obtaining personal identifying information about their victims, often buying it online from other criminals. They use this stolen information to impersonate their victims, convincing a cellphone company to reassign a victim's phone number to the SIM card in the criminal's phone. (SIM is short for Subscriber Identity Module, which includes a unique ID number for a specific mobile phone account.) The scammers then break into the victim's online financial accounts—typically logging in with stolen usernames and passwords. They intercept security codes sent to the victim's cellphone number via text or call. They then reset passwords to lock victims out.

21% of Americans
(56 MILLION U.S. ADULTS) WERE DEFRAUDED OUT OF $25.4 BILLION IN TELEPHONE SCAMS IN 2023.
—TRUECALLER'S LATEST EDITION OF THE "U.S. SPAM AND SCAM REPORT"

Once in control of your phone, they rob you blind. "When a SIM swap attack happens, the end goal is your money," says Jonathan S. Weissman, cybersecurity principal lecturer at Rochester Institute of Technology.

Losses can be devastating. SIM swappers stole $65,000 from a California man's bank account and drained a Florida woman's life savings of over $68,000 in 2022, according to news reports. In February, three members of a criminal gang called the Powell SIM Swapping Crew were indicted in U.S. District Court on charges they stole more than $400 million in crypto between 2021 and 2023 from over 50 victims in more than a dozen states.

In April, reports surfaced online that scammers attempted to bribe cellphone company employees to make the swaps.

The Federal Communications Commission vows to curb the problem with rules that will go into effect this year requiring carriers to protect customers from SIM swaps. But cybersecurity experts say you can take steps now to protect yourself.

► Freeze your phone number. Ask your cellphone carrier if you can lock or freeze your phone number so a secret password or PIN must be provided before the carrier will make changes to the account. The FCC will require carriers to offer locking or freezing soon, but you can ask for it before rules go into effect.

► Act fast if you recognize a SIM swap. If your cellphone suddenly won't connect to your provider and you cannot make calls or receive text messages, you may be the victim of a SIM swap, the FCC warns. Use your landline or a borrowed phone to call your cellphone provider. Contact your bank and other financial institutions right away to make sure accounts haven't been breached.

► Don't rely on text messaging for account security codes. Multifactor authentication for bank, credit card, email and other accounts often means getting a code via text message when you log in. But if a bad actor is in control of your phone number, they'll get those secret codes, says security researcher Kevin Lee, lead author of a SIM swap study by Princeton University. When possible, use an authenticator app.

► Beef up usernames and passwords. Use strong, unique usernames and passwords, Weissman advises. "A long password that you never reuse on other accounts is best," he says.

► Hide personal info. Don't make yourself a target. Keep quiet on social media about personal details such as your date of birth, mom's maiden name, your first car and where you went to elementary school, the wireless trade group CTIA recommends.

Sari Harrar is a contributing editor at AARP who writes frequently about health and fraud.

Have questions related to scams? Call the AARP Fraud Watch Network helpline toll-free at 877-908-3360. For the latest fraud news and advice, go to aarp.org/fraudwatchnetwork.

CHRIS GASH