THE WALL STREET JOURNAL.

https://www.wsj.com/articles/how-safe-is-your-mobile-phone-not-as-safe-as-you-think-11559700420

JOURNAL REPORTS: TECHNOLOGY

How Safe Is Your Mobile Phone? Not as Safe as You Think

Three experts talk about where the weaknesses are—and what companies can do about it

Attackers can use a type of fraud known as a SIM swap to gain entry into a victim's most sensitive online accounts. PHOTO: ISTOCK

By Drew FitzGerald

June 4, 2019 10:07 pm ET

Websites and apps often ask for users' phone numbers to enhance their security. Those digits allow two-factor authentication: After a user types in a password, the website sends a text message to verify the login attempt is legitimate—the second factor.

This method protects millions of users from theft, but it isn't foolproof.

A common type of mobile-phone fraud is known as a SIM swap, so named for the subscriber identity module inside a smartphone that identifies its owner. Criminals who gather details about a victim can sometimes persuade a wireless company to transfer a phone number to a new phone. Attackers can then trick banks and other companies into granting a password reset sent to a new phone, enabling them to gain entry into a victim's most sensitive online accounts.

JOURNAL REPORT

- Read more at WSJ.com/journalreporttech

MORE IN CYBERSECURITY

- The Quantum Threat to Encryption
- Our Emotional Attachment to Our Passwords
- Can the Sound of Your Typing Be Decoded?
- The Tussle Over Facial Recognition

Relying on phone numbers means that a single, often publicly available, piece of information is becoming a crucial part of our identities. And that, in turn, raises some difficult questions. Should people be concerned about relying on text-message-based, two-factor authentication? Are our phone numbers taking on a job they weren't designed for? Is there any alternative?

The Wall Street Journal spoke with three experts in mobile security: Allison Nixon, director of security research at Flashpoint, a business intelligence provider; Jim Greenwell, former chief of Danal, an authentication service for online financial transactions; and Cathal Mc Daid, the chief technology officer at Adaptive Mobile, a security firm that serves telecom companies.

Here are edited excerpts of the conversation:

Hacking attacks

WSJ: *Tell us about phone-hacking attacks, such as tricking someone either online or on the phone and in some way abusing their trust.*

MR. MC DAID: One very popular way of doing it is that you ring up the carrier and you say, "My name is X and my phone number is X. However, I've lost my SIM card or it's been damaged or been destroyed somehow and I need to get it assigned to a new phone."

WSJ: *Is the SIM card itself hackable?*

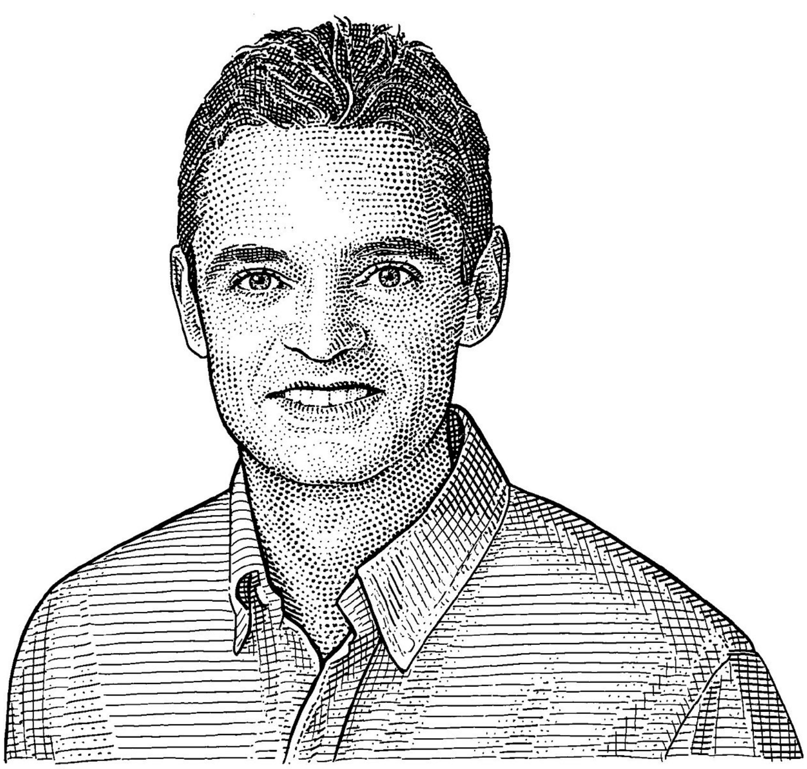
MS. NIXON: When I look at all the hacks that are going on, they are not around the SIM card technology itself.

SIM swapping is a fraud technique used to basically abuse the way mobile authentication works nowadays. A lot of online providers will set up mass [two-factor authentication], but more important, they also add SMS password reset onto accounts.

A victim might add a phone number to their account either for verification or to set up a two-factor, but then the provider will silently also add password reset as an option. And the user almost never knows about this, unfortunately.

When the SIM swappers steal a phone number, for that very short period of time they own the victim's phone number. Then they do a password reset against their emails until they take over the victim's financial accounts and steal what they want.

The technique has existed for many years now. In the past two years, it really blew up with stealing cryptocurrency accounts. In the past half year or so, they've kind of run out of cryptocurrency victims, and we're seeing regular bank accounts getting cleaned out now, unfortunately.



Cathal Mc Daid

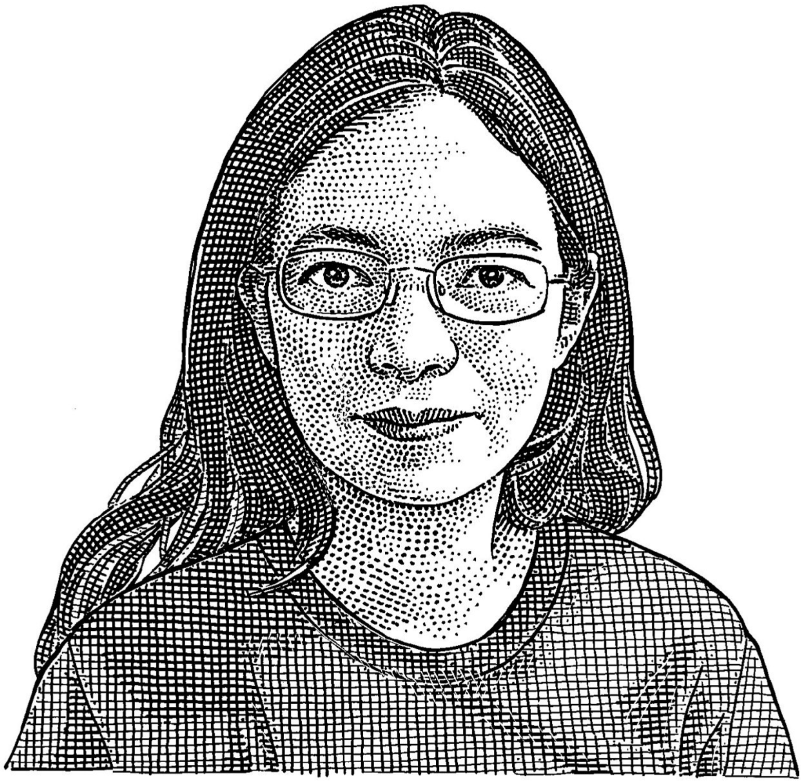
Who should worry?

WSJ: *The vast majority of people haven't seen these types of attacks happen to them. Is this something that the average person should worry about?*

MR. MC DAID: It depends. I know that is a terrible answer but it depends really on what they use. I think for anybody using cryptocurrencies, I would definitely recommend that they review how it's all set up and the security behind it. But the reason why you don't see tens of thousands of people being affected is it takes work from the attackers to actually do this. It isn't something they can do in bulk, like it has happened for credit-card hacks, where you can access everybody's information in one fell swoop.

MS. NIXON: I don't see a situation where people *don't* have to worry. I see a situation where threat actors are building capabilities, increasing the number of SIM swaps they do over time. And we're seeing, increasingly, regular people getting robbed from their retirement account. It isn't just rich people, it's not just cryptocurrency people.

Nowadays, these techniques are spreading to more and more criminal gangs. We're also seeing organized, well-funded attempts to recruit phone-company employees. I don't think that they're ever going to run out of candidate employees, because you have thousands and thousands of phone-company retail employees making retail wages, and they're being bribed with a couple of hundred dollars or more per SIM swap. You're going to have at least one or two people bite when you have these recruitment operations going in a systematic manner.



Allison Nixon

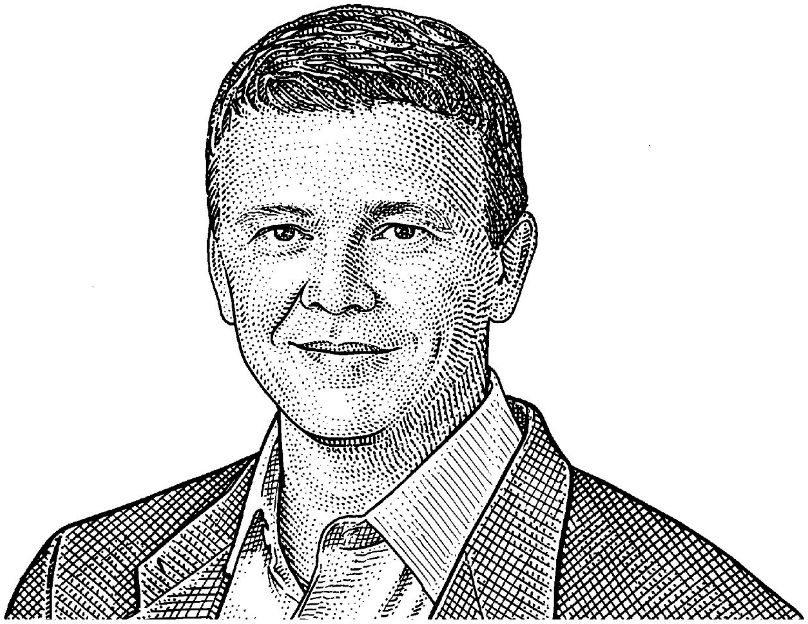
Best solution

WSJ: *So what's the best solution? Is there something that can be patched or fixed with new standards?*

MS. NIXON: Unfortunately, I think there is not going to be any way to prevent a SIM swap from happening. The way to remediate this is probably going to be on the other end. [Businesses using text messages in two-step verification] need to properly validate that a SIM swap didn't happen.

MR. GREENWELL: There is no single solution to fraud. Fraudsters get creative. It seems that the industry is going toward a layered approach, meaning not only the mobile device. But you may have biometrics or behavioral identity—you can tell how I hold my phone, how quickly I respond to things, my heartbeat, all those types of things.

But remember, the benefits are balanced by friction for the consumer. Most transactions—you're talking about billions of transactions a day—are legitimate and you don't want to make it extra tough for the customer.



Jim Greenwell

I can assure you I could stop all fraud tomorrow—it just wouldn't be a very friendly customer experience.

MS. NIXON: There are countermeasures for SIM swapping that can make it almost impossible to take over people's accounts. But it would cause friction for the customer. For example if [banks'] policy required a period of time to pass [after a password was reset] before you could empty out an account, that would definitely prevent SIM swapping. The attackers can only hold on to a phone number until the victim gets it back—usually not that long. However, most of the time when people are doing password resets, it's legitimate, and when you lock down an account for a period of time it makes people very frustrated.

Some other countries have implemented fixes that have pretty much fixed the problem and haven't increased customer friction in any noticeable way. There are some countries in Africa where telecom providers operate public webpages where you can query a phone number and receive back a yes/no answer on whether there was a hardware change or ownership change within the past few days. And then web mail providers, banks and so forth can query that portal and find out if there is something weird going on with that phone number.

Something like that is probably worthwhile for U.S. carriers to consider. Such a webpage would be open for any website out there to use for its authentication purposes, with a minimal exposure of personal information.

MR. MC DAID: The International Telecommunication Union, the U.N. standards body, is releasing a paper soon about how to prevent this type of [SIM-swap scam] activity. Some of that involves regulatory and internal rules on SIM swaps, including linking banks and operators' databases to help determine if a SIM swap has occurred. And that comes down to using things like the IMEI [a unique number that is assigned to each phone]. These could be used to determine if a SIM swap has occurred, i.e., an indication of suspicion is if the reason given is a damaged SIM, but then a different handset is used with the "replacement'' SIM.

MS. NIXON: It's tough, though. As a third party you can't get access to such numbers because that is considered private. So it's really up to the phone companies to open up some level of information so that third parties can actually use phone numbers as a proper identifier.

The process used by those countries in Africa seems like the best way to go. It's a minimal exposure of personal data, it's accessible to everyone, and it doesn't increase friction except in narrow situations where it should. But it won't make anyone rich.

MR. MC DAID: It seems that everybody can see there is value in having a coordinated system, but deciding who or what is going to create any system, manage it and pay for it is not clear-cut.

WSJ: *Is there anything else the public should know about the risk of fraud through mobile devices?*

MS. NIXON: I think the public needs to pressure companies they do business with to do a better job at authentication. Account security advice handed out by providers not only tends to place the burden of responsibility, and blame, solely on the user—but it is increasingly tone-deaf when account takeovers are the result of a provider's error.

The public also needs to understand that our country lacks any truly effective mechanism for people to prove their identities online, which enables an incredible amount of fraud and is a bigger problem than any one provider can tackle themselves.

Mr. FitzGerald is a reporter for The Wall Street Journal in Washington, D.C. He can be reached at andrew.fitzgerald@wsj.com.

Appeared in the June 5, 2019, print edition.