anuary 05, 2023

**What is SIM swapping & how does the hijacking scam work?**

SIM swapping, also known as SIM splitting, simjacking, or SIM hijacking, is a technique used by fraudsters to get control of your phone number. With your phone number, hackers can take advantage of two-factor authentication to gain access to your bank accounts, social media accounts, and more.

**To understand SIM swapping, you first have to know how two-factor authentication and SIM cards work.**

**Security experts recommend** [**two-factor authentication**](https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/importance-of-two-factor-authentication) to protect your online accounts, but it isn’t a perfect system – a third party with your phone number could bypass it. Two-factor authentication alone doesn’t 100% protect your accounts from getting hacked.

Setting up two-factor authentication for an account typically entails providing your cell phone number, so that you can receive unique codes to use each time you log in after entering your username and password. The code may also be sent to your email. Since two-factor authentication has become so common, hackers now have another challenge to gaining access to your information – they now need to get your cell phone number, too.

A person wearing a mask

Description automatically generated

**What is a SIM card?**

“SIM” stands for “subscriber identity module.” A SIM card is a tiny chip inserted inside your cell phone. Your SIM card has a unique string of numbers assigned to it that identify the user, mobile carrier, and country of the cell phone. SIM cards are also connected to your phone number.





**Microsoft Defender**

Stay safer online with one easy-to-use app1  
  
1Microsoft 365 Personal or Family subscription required; app available as separate download

[**Learn more**](https://www.microsoft.com/en-us/microsoft-365/microsoft-defender-for-individuals?ocid=cmmfl4v07qv)

**How does SIM swapping work?**

To get your phone number, scammers must contact your mobile carrier and convince them to transfer your phone number to one of their own SIM cards. But mobile carriers don’t transfer cell phone numbers just because someone asks – they require more information to do so.

Fraudsters often use social media to collect personal information they could use to answer security questions to gain access to their target’s account. For example, your birthday, your mother’s maiden name, and the high school you went to are common security questions that a third party could easily get the answers to by browsing your social media.

Another way scammers can gather your personal information is through phishing. Phishing is a form of [**social engineering**](https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-social-engineering) where attackers impersonate a trusted institution or individual to get you to share your personal information. For example, scammers may send an email that appears to be from your phone carrier, asking you to keep your account information updated. To do so, they may ask you to click a link and log in, and capture your information in the process. These convincing emails trick victims into sharing personal information like their birthday, password, account number, and more.

Sometimes, scammers even purchase victims’ personal information from sellers of leaked and stolen data on the [**dark web**](https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web).

Once the scammers gather your information, they will contact your mobile carrier. If they can successfully answer your security questions, their next step is to get your phone number transferred to their SIM card. Then, they can get into your online accounts using authentication codes sent to your phone number, which they now have control over.

**SIM swap detection**

<="" p="" style="box-sizing: inherit; margin-top: 0px; margin-bottom: 0px; clear: both; font-size: 15px; line-height: 20px; padding: 24px 0px 0px; font-weight: 400; font-family: "Segoe UI", SegoeUI, "Helvetica Neue", Helvetica, Arial, sans-serif; color: rgb(0, 0, 0); font-style: normal; font-variant-ligatures: normal; font-variant-caps: normal; letter-spacing: normal; orphans: 2; text-align: start; text-indent: 0px; text-transform: none; widows: 2; word-spacing: 0px; -webkit-text-stroke-width: 0px; white-space: normal; background-color: rgb(255, 255, 255); text-decoration-thickness: initial; text-decoration-style: initial; text-decoration-color: initial;">

* **You can’t send or receive text messages or make phone calls**

Being unable to send or receive text messages or make or receive phone calls is a telltale sign that you’re a victim of SIM swapping. This is because scammers are now in control of your phone number.

* **Losing phone service**

If your phone is giving you a “No Service” or “Searching” message, that is another way SIM swapping can be detected.

* **You’re notified your phone number is on a new device**

For security purposes, mobile carriers often notify their customers when their SIM card or phone number was activated on a new device.

* **Strange activity on social media**

If you’re noticing unusual activity on social media accounts, that may be the result of SIM card hacking. Hackers may use SIM swapping to get into your social media accounts to impersonate you and [**scam**](https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/whats-a-scam-and-whats-real) your friends or family members for money.

* **You can’t access your accounts**

Hackers often change your login credentials immediately so they can take full control over the account.

* **You notice unusual bank activity**

If you notice purchases, wire transfers, or withdrawals that you don’t recall making, your SIM card could have been hacked. Gaining access and using victims’ funds is often the ultimate goal for SIM swappers.

**How to protect yourself from SIM swapping**

Follow these tips to secure your SIM card, as well as your personal information, to prevent SIM hijacking.

**Use the internet wisely**

Fraudsters will use [**phishing techniques**](https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/spear-phishing-attack) to steal your personal information. It’s important that you get to know these techniques.

Don’t click on links from people you don’t know. Organizations like your phone carrier or bank will never ask for your sensitive information via email.

Additionally, you may want to consider making your social media accounts private. Avoid sharing too much personal information that scammers can use to impersonate you online.

**Update your account security**

Some mobile carriers allow their customers to set up a special PIN number that must be entered to make changes to their accounts. If your mobile carrier allows this, it’s wise to take them up on it. Don’t make your PIN number something obvious that a hacker could figure out, like your birthday. You also may want to create a stronger password for your cellphone’s account, and choose more difficult security questions and answers.

**Use an authentication app**

[**Authentication apps**](https://www.microsoft.com/en-us/security/mobile-authenticator-app) use two-factor authentication that is linked to your device, rather than your phone number—so if you’ve got your phone, this form of authentication is still protected even if a hacker’s able to intercept your calls and texts.

**Sign up for alerts**

Check to see if your mobile carrier offers extra alerts for events like a phone number or SIM card change. If your mobile carrier gives you that option, you should turn on the notifications.

Your phone number and SIM card are used for more than just keeping in touch with your friends – they’re also play a huge role in your online security. Now that you’ve read all about SIM swapping, you’ve taken a huge step in protecting your personal information.

[What is SIM swapping & how does the hijacking scam work? – Microsoft 365](https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-sim-swapping?msockid=01ce7eab54b961a71b716bb055b960bf)

What is Sim swap fraud?

Is where a criminal pretends to be yourself or a mobile operator and tries to your mobile phone network that you need a replacement Sim for your phone.

This lets them take control of your mobile phone number, which means they can potentially hijack your calls and texts, as well as your online banking details/codes.

Things to look out for

You've lost the ability to make calls or texts

This is one of the first sign that you could be a victim of SIM swapping. This could mean fraudsters have deactivated your SIM and are using your phone number.

You receive a notification of activity elsewhere

If your phone provider notifies you that your SIM card or phone number has been activated on a different device.

You lose access to accounts

If your login credentials suddenly no longer work for things like your banking sites. Contact your bank and other organizations immediately.

Steps to protect yourself

SIM swaps will be conducted by your phone providers either via requests in their shops, on their websites or verbally via their call centres.

1. 1

Don't respond to fake emails, text or phone calls, These are ways in which fraudsters use to gather personal information about you

1. 2

Be careful what you share on social media, Avoid posting things about yourself or family members birthdates, pet names and schools as these are often questions used to reset passwords.

1. 3

If your phone suddenly stops working then inform both your bank and mobile network

1. 4

Use unique passwords that only you will know

--

* [**What Is a SIM-Swap Attack?**](https://www.howtogeek.com/668922/how-to-protect-yourself-from-sim-swapping-attacks/#what-is-a-sim-swap-attack)
* [**Who Is Most at Risk?**](https://www.howtogeek.com/668922/how-to-protect-yourself-from-sim-swapping-attacks/#who-is-most-at-risk)
* [**How Do You Know an Attack Has Taken Place?**](https://www.howtogeek.com/668922/how-to-protect-yourself-from-sim-swapping-attacks/#how-do-you-know-an-attack-has-taken-place)
* [**How Should You Respond to a SIM-Swapping Attack?**](https://www.howtogeek.com/668922/how-to-protect-yourself-from-sim-swapping-attacks/#how-should-you-respond-to-a-sim-swapping-attack)
* [**How to Protect Yourself From an Attack**](https://www.howtogeek.com/668922/how-to-protect-yourself-from-sim-swapping-attacks/#how-to-protect-yourself-from-an-attack)

**Key Takeaways**

* **SIM swapping is a method hackers use to bypass two-factor authentication (2FA) by tricking phone companies into transferring a phone number to a new SIM card.**
* **SIM-swapping attacks are mainly financially motivated and cryptocurrency accounts have become popular targets due to the lack of chargeback options.**
* **If you suspect a SIM-swapping attack, take immediate action to secure your bank accounts and credit lines, change your passwords, and contact the police to file a report. Prevention includes using app-based authentication or physical security keys, rather than SMS-based 2FA.**

You think you’re making all the right moves. You’re smart with your security. You have [two-factor authentication](https://www.howtogeek.com/117047/why-you-should-use-two-factor-authentication-2fa/) enabled on all your accounts. But hackers have a way to bypass that: SIM swapping.

*This*[*Cybersecurity Awareness Week*](https://www.howtogeek.com/tag/cybersecurity-week-2023/)*article is brought to you in association with [Incogni](https://www.howtogeek.com/g/QmhiPb" \t "_blank) .*

**What Is a SIM-Swap Attack?**

There’s nothing inherently wrong with "SIM swapping." If you ever lose your phone, your carrier will perform a SIM swap and move your cell phone number to a new SIM card. It’s a routine customer service task.

The problem is hackers and organized criminals have figured out how to trick phone companies into performing SIM swaps. They can then access accounts protected by [SMS-based two-factor authentication](https://www.howtogeek.com/361244/sms-two-factor-auth-isn%E2%80%99t-perfect-but-you-should-still-use-it/) (2FA).

Suddenly, your phone number is associated with someone else's phone. The criminal then gets all text messages and phone calls intended for you.

Two-factor authentication was conceived in response to the problem of leaked passwords. Many sites fail to properly protect passwords. They use hashing and salting to prevent passwords from being read in their original form by third-parties.

Even worse, many people reuse passwords across different sites. When one site gets hacked, an attacker now has everything he needs to attack accounts on other platforms, creating a snowball effect.

For security, many services require that people provide a special one-time password (OTP) whenever they log in to an account. These OTPs are generated on the fly and are only valid once. They also expire after a short time.

For convenience, many sites send these OTPs to your phone in a text message, which has its own risks. What happens if an attacker can obtain your phone number, either by stealing your phone or performing a SIM swap? This gives that person almost unfettered access to your digital life, including your banking and financial accounts.

So, how does a SIM-swap attack work? Well, it hinges on the attacker tricking a phone company employee into transferring your phone number to a SIM card he or she controls. This can happen either over the phone, or in-person at a phone store.

To accomplish this, the attacker needs to know a bit about the victim. Fortunately, social media is filled with the biographical details likely to fool a security question. Your first school, pet, or love, and your mother’s maiden name can all likely be found on your social accounts. Of course, if that fails, there’s always [phishing](https://www.howtogeek.com/437513/what-should-you-do-if-you-receive-a-phishing-email/).

SIM-swapping attacks are involved and time-consuming, making them better-suited for targeted incursions against a particular individual. It’s hard to pull them off at scale. However, there have been some examples of widespread SIM-swapping attacks. One Brazilian organized crime gang was [able to SIM swap 5,000 victims](https://www.uol.com.br/tilt/noticias/redacao/2018/12/10/clonagem-no-whatsapp-mais-de-5-mil-ja-sofreram-este-golpe-no-brasil.htm) over a relatively short period of time.

A ["port-out" scam](https://www.howtogeek.com/342988/what-is-a-phone-port-out-scam-and-how-can-i-protect-myself/) is similar and involves hijacking your phone number by "porting" it to a new cellular carrier.

**Who Is Most at Risk?**

Hannah Stryker / How-To Geek

Due to the effort required, SIM-swapping attacks tend to have particularly spectacular outcomes. The motive is almost always financial.

Recently, [cryptocurrency](https://www.howtogeek.com/141374/htg-explains-what-is-bitcoin-and-how-does-it-work/) exchanges and wallets have been popular targets. This popularity is compounded by the fact that, unlike traditional financial services, there’s no such thing as a chargeback with Bitcoin. Once it’s sent, it’s gone.

Furthermore, anyone can create a cryptocurrency wallet without having to register with a bank. It’s the closest you can get to anonymity where money is concerned, which makes it easier to launder stolen funds.

One well-known victim who learned this the hard way is [Bitcoin investor, Michael Tarpin](https://markets.businessinsider.com/currencies/news/bitcoin-investor-loses-24-million-of-crypto-sim-swap-hackers-2019-11-1028677818), who lost 1,500 coins in a SIM-swapping attack. This happened mere weeks before Bitcoin hit its all-time highest value. At the time, Tarpin's assets were worth over $24 million.

When ZDNet journalist, Matthew Miller, [fell victim to a SIM-swap attack](https://www.zdnet.com/article/sim-swap-horror-story-ive-lost-decades-of-data-and-google-wont-lift-a-finger/), the hacker tried to purchase $25,000 worth of Bitcoin using his bank. Fortunately, the bank was able to reverse the charge before the money left his account. However, the attacker was still able to trash Miller's entire online life, including his Google and Twitter accounts.

Sometimes, the purpose of a SIM-swapping attack is to embarrass the victim. This cruel lesson was learned by Twitter and Square founder, Jack Dorsey, on August 30, 2019. Hackers [hijacked his account](https://www.businessinsider.com/jack-dorsey-hack-sim-swapping-how-2019-8?utm_source=markets&utm_medium=ingest) and posted racist and anti-Semitic epithets to his feed, which is followed by millions of people.

**How Do You Know an Attack Has Taken Place?**

The first sign of a SIM-swapping account is the SIM card loses all service. You won’t be able to receive or send texts or calls, or access the internet through your data plan.

In some cases, your phone provider might send you a text informing you that the swap is taking place, moments before moving your number across to the new SIM card. [This is what happened to Miller:](https://www.zdnet.com/article/sim-swap-horror-story-ive-lost-decades-of-data-and-google-wont-lift-a-finger/)

*"At 11:30 pm on Monday, 10 June, my oldest daughter shook my shoulder to wake me up from a deep sleep. She said that it appeared my Twitter account had been hacked. It turns out that things were much worse than that.*

*After rolling out of bed, I picked up my Apple iPhone XS and saw a text message that read, 'T-Mobile alert: The SIM card for xxx-xxx-xxxx has been changed. If this change is not authorized, call 611.'"*

If you still have access to your email account, you might also start to see strange activity, including notifications of account changes and online orders you didn’t place.

**How Should You Respond to a SIM-Swapping Attack?**

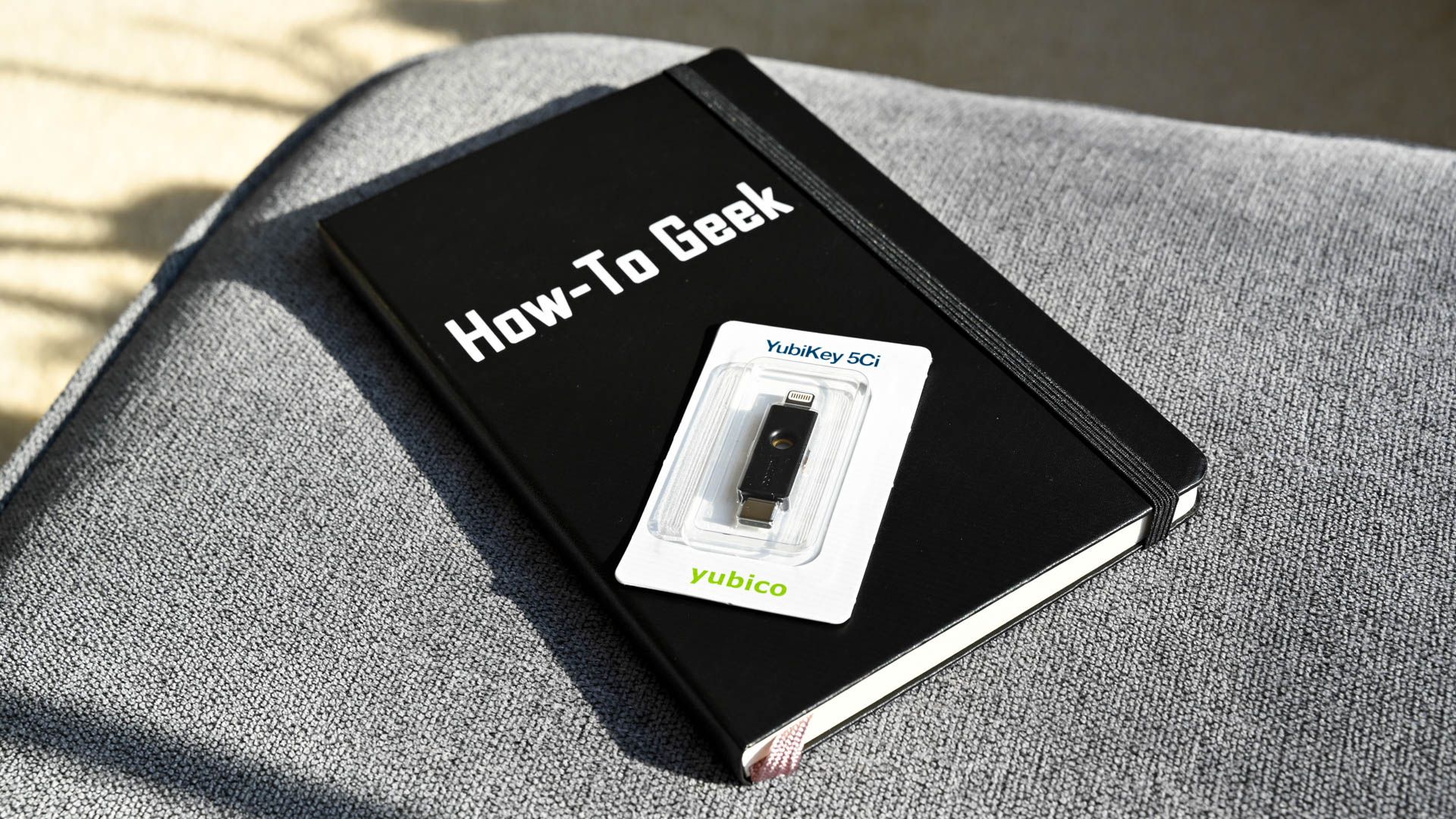
When a SIM-swapping attack happens, it’s crucial you take immediate, decisive action to prevent things from getting worse.

First, call your bank and credit card companies and request a freeze on your accounts. This will prevent the attacker from using your funds for fraudulent purchases. Since you’ve also effectively been the victim of identity theft, it's also wise to contact the various credit bureaus and request a freeze on your credit.

Then, try to "get ahead" of the attackers by moving as many accounts as possible to a new, un-tainted email account. Unlink your old phone number, and use strong (and completely new) passwords. For any accounts you're unable to reach in time, contact customer service.

Finally, you should contact the police and file a report. I can’t say this enough — you’re the victim of a crime. Many homeowner's insurance policies include protection for identity theft. Filing a police report might allow you to file a claim against your policy and recover some money.

**How to Protect Yourself From an Attack**

Hannah Stryker / How-To Geek

Of course, prevention is always better than a cure. The best way to protect against SIM-swapping attacks is to [simply not use SMS-based 2FA](https://www.howtogeek.com/310418/why-you-shouldnt-use-sms-for-two-factor-authentication/). Fortunately, [there are some compelling alternatives](https://www.howtogeek.com/232598/5-different-two-step-authentication-methods-to-secure-your-online-accounts/).

You can use an app-based authentication program, like Google Authenticator. For another level of security, you can choose to purchase a physical authenticator token, like the YubiKey or Google Titan Key.

If you absolutely must use text- or call-based 2FA, you should consider investing in a dedicated SIM card you don’t use anywhere else. Another option is to use a Google Voice number, although that isn’t available in most countries.

Unfortunately, even if you use app-based 2FA or a physical security key, many services will allow you to bypass these and regain access to your account via a text message sent to your phone number. Services like Google Advanced Protection offer more bulletproof security for people at risk of being targeted, ["like journalists, activists, business leaders, and political campaign teams."](https://www.howtogeek.com/404450/what-is-google-advanced-protection-and-who-should-use-it/)

An unfortunate number of services only allow SMS or voice call based 2FA at this time, including many banks, so it is well worth being prepared for such an attack.

Sen initial One

SIM swapping is a technique used by attackers to take control of a victim’s phone number. This guide explores how SIM swapping works, its implications for security, and strategies for prevention.

Learn about the importance of securing personal information and using multi-factor authentication. Understanding SIM swapping is crucial for protecting against identity theft and fraud.

SIM swapping attacks represent a vulnerability in [two-factor authentication](https://www.sentinelone.com/cybersecurity-101/what-is-multi-factor-authentication-mfa/) (MFA/2FA). As a result, it has led to high-profile breaches, financial losses, and identity theft cases. In the current threat landscape, SIM swapping has become an attractive tool for hackers seeking to infiltrate cryptocurrency wallets, social media accounts, and financial institutions.

A close-up of a phone

Description automatically generated

**A Brief Overview & History of SIM Swapping**

SIM swapping, a term that has garnered increasing notoriety in recent years, is a sophisticated and malicious technique employed by cybercriminals to gain unauthorized access to a victim’s mobile phone number and subsequently infiltrate sensitive accounts and data. It involves convincing a mobile carrier to transfer the victim’s phone number to a SIM card under the attacker’s control, thereby providing the attacker with the ability to intercept SMS-based two-factor authentication codes and reset [passwords](https://www.sentinelone.com/cybersecurity-101/password-security-business-tips/). This seemingly straightforward yet devastatingly effective tactic exploits the trust that mobile carriers have historically placed in customers’ requests for SIM card changes, making it a serious vulnerability in the security landscape.

The origins of SIM swapping can be traced back to the mid-2000s when it was primarily a tool used by [hackers](https://www.sentinelone.com/cybersecurity-101/what-is-a-hacker/) and scammers to engage in identity theft and wire fraud. Over the years, the technique has evolved, becoming more sophisticated and refined. Nowadays, it has emerged as a pervasive and damaging threat to individuals, businesses, and even high-profile personalities. Its usage has expanded from simply gaining unauthorized access to email or social media accounts to infiltrating cryptocurrency wallets, where attackers can steal vast sums of digital currency. Moreover, it is employed in financial fraud, online banking, and other [malicious activities](https://www.sentinelone.com/cybersecurity-101/what-is-malware-detection/), often with far-reaching consequences.

**Understanding How SIM Swapping Works**

SIM swapping begins with the attacker identifying a target. This might involve researching the victim online to find personal information, including their mobile phone number, carrier, and even answers to security questions.

Armed with this information, the attacker initiates a [social engineering](https://www.sentinelone.com/cybersecurity-101/what-is-social-engineering/) campaign. They impersonate the victim and contact the victim’s mobile carrier’s customer support. They may use various tactics to convince the carrier that they are the account holder and need a new SIM card. Common tactics include pretending to have lost the original SIM card or claiming to need a replacement for a damaged card.

Once the attacker successfully contacts the carrier, they provide the victim’s information, including the mobile phone number and any additional details that may be requested. If the attacker is convincing enough, the carrier may issue a new SIM card without properly verifying the caller’s identity.

With the new SIM card in hand, the attacker inserts it into a device they control. This device is often a spare phone or a SIM card reader/writer. The attacker then activates the new SIM card, essentially taking over the victim’s phone number.

Once the victim’s phone number is under the attacker’s control, they can intercept SMS messages and phone calls. This is where the real damage can occur. If the victim uses SMS-based 2FA, the attacker can receive the authentication codes sent to the victim’s number, granting them access to the victim’s accounts. The attacker can also use the stolen phone number to reset passwords for various accounts, taking over email, social media, and financial accounts.

With access to the victim’s accounts, the attacker can engage in a range of malicious activities, from stealing sensitive information and funds to conducting identity theft and fraud. To avoid detection, attackers may attempt to lock the victim’s SIM card or otherwise disrupt the victim’s access to their phone number. They may also quickly change account recovery options, making it harder for the victim to regain control.

It’s important to note that SIM swapping is not a guaranteed success for attackers. Mobile carriers are increasingly implementing more robust authentication and verification procedures to prevent such attacks. For instance, they might require additional security questions or a physical visit to a store for SIM card replacement. However, it remains a significant concern due to the potential harm it can cause.

**Exploring the Use Cases of SIM Swapping**

Perhaps the most well-documented use of SIM swapping is its role in cryptocurrency theft. Cybercriminals target individuals known to hold substantial cryptocurrency assets and use SIM swapping to gain control of their mobile numbers. Once in control, they intercept two-factor authentication codes and gain access to cryptocurrency wallets, resulting in significant financial losses. The significance of these attacks lies in the substantial financial stakes involved and the relatively irreversible nature of cryptocurrency transactions.

SIM swapping has also been utilized to hijack high-profile social media accounts. Hackers gain control over a victim’s phone number to reset passwords, effectively taking over their social media profiles. This can lead to reputational damage, spread misinformation, and even have broader societal implications when influential figures are targeted.

In more generalized instances, SIM swapping is used for identity theft and financial fraud. Attackers compromise victims’ mobile numbers, access email accounts, and manipulate password resets to infiltrate bank accounts, credit cards, and online services. The consequences extend to financial loss, compromised personal information, and reputational damage.

SIM swapping can also lead to the unauthorized access of sensitive business information. For individuals working in corporate environments, having their mobile number compromised can provide hackers with access to corporate email accounts and other sensitive data. This presents a significant security risk for businesses, particularly if employees have access to proprietary or confidential information.

In response to the escalating threat of SIM swapping, businesses and individuals are taking proactive measures to secure against its risks:

* Enhanced Authentication Methods – One of the most crucial steps is moving away from SMS-based two-factor authentication (2FA) and adopting more secure methods, such as time-based one-time passwords (TOTP) generated by authenticator apps or hardware tokens. These methods are not reliant on SMS, making it significantly more challenging for attackers to intercept authentication codes.
* Account Recovery Protocols – Individuals and businesses are revisiting their account recovery options. Rather than relying solely on mobile numbers for account recovery, they are adding alternative methods, like backup email addresses and security questions. This adds an extra layer of security, making it more difficult for attackers to take control of accounts.
* Mobile Carrier Security Measures – Mobile carriers are increasingly implementing stronger identity verification processes before issuing a new SIM card or transferring phone numbers. They are also working on improving their customer support training to detect and prevent fraudulent SIM swap attempts. Additionally, some carriers offer services that allow customers to set up PINs or passphrases to protect their accounts from unauthorized changes.
* Security Awareness and [Education](https://www.sentinelone.com/cybersecurity-101/cybersecurity-training/) – Raising awareness about SIM swapping and its risks is crucial. Both businesses and individuals need to educate themselves and their employees about the potential threats and how to protect against them. Regular security training and reminders about best practices can go a long way in reducing the risk of falling victim to SIM swapping attacks.

**Conclusion**

SIM swapping has emerged as a serious and evolving threat in the digital age, with real-world use cases that demonstrate its potential for financial loss, reputational damage, and compromised security. The response to this threat involves the adoption of more secure authentication methods, robust account recovery protocols, cooperation with mobile carriers, and ongoing security awareness efforts, all aimed at mitigating the risks associated with SIM swapping.

[What is SIM Swapping? - SentinelOne](https://www.sentinelone.com/cybersecurity-101/threat-intelligence/what-is-sim-swapping/)