
# SIM-swapping Attacks Explained

In recent years, a growing number of organizations have implemented stronger cybersecurity measures, including multifactor authentication (MFA). This method requires a user to present two or more unique credentials, such as a password and an additional security code, to verify their identity and log into their company account. With MFA, cybercriminals will still be restricted from infiltrating organizations' IT infrastructures upon stealing users' passwords, as they will lack the extra credentials required for access. Although this cybersecurity tactic has proven useful for many organizations, some cybercriminals have figured out a way to exploit MFA through users' subscriber identity module (SIM) cards. These cards are an essential component of any cellphone, as they unlock a host of information and services (e.g., the user's contacts and texting and calling capabilities). By transferring their SIM card to another phone, a user can automatically shift their existing mobile profile to the new device.

Unfortunately, some cybercriminals have begun tricking mobile carriers into transferring users' profiles to SIM cards on their own devices, thus giving them unauthorized access to users' cellphone activities. Because the additional security codes required for MFA are often sent via text, cybercriminals with fraudulent SIM cards can complete users' extra account verification steps with ease and go on to infiltrate company networks, data and funds. According to the FBI, this technique, also known as SIM swapping, generated nearly $50 million in losses in the past year alone. As such, it's important for organizations to understand SIM-swapping attacks and how to prevent and respond to them.

## How SIM-swapping Attacks Work

A SIM-swapping attack generally consists of the following steps:

- **Gathering the user's personal information**—First, a cybercriminal collects a variety of personal details about their target, such as their name, date of birth, contact information and employment history. The cybercriminal likely gathers these details by reviewing the user's online profiles or tricking them into sharing this information via deceptive messages, malicious links or other social engineering tactics.
- **Manipulating the mobile carrier**—After gathering their target's personal details, the cybercriminal leverages this information to persuade the user's mobile carrier to conduct the SIM swap. This may occur in one of two ways: The cybercriminal contacts the carrier while pretending to be the target and asks that the user's phone number and mobile profile be transferred to a new SIM card, or the cybercriminal utilizes social engineering tactics to hack into the target's mobile profile and connect the user's phone number to a different SIM card by themself, bypassing the carrier altogether. From there, the cybercriminal receives the user's texts, calls and other cellphone services on their own device.
- **Exploiting MFA**—Following the SIM swap, the cybercriminal is able to intercept their target's MFA-related requests. For example, the cybercriminal may receive a text containing an additional security code, also called a one-time passcode, on their SIM-swapped device, which allows them to successfully log into the user's company account.
- **Compromising company information and assets**—Upon exploiting MFA and logging into their target's account, the cybercriminal is able to compromise company data and resources in various ways. This may include causing network disruptions, damaging or exposing sensitive information, and stealing company funds or intellectual property. These actions could have lasting impacts on the affected user and organization, resulting in large-scale losses.
- **Reversing the swap**—In some cases, the target and affected organization can detect the SIM-swapping attack immediately or shortly after it occurs. However, if this isn't the case, the cybercriminal may contact the mobile carrier or resort to their own hacking methods to reverse the SIM swap. Depending on how quickly the cybercriminal accomplishes this, they may be able to avoid alerting the user that the swap took place and allow the attack to go unnoticed for some time.

SIM-swapping attacks are usually carried out by external cybercriminals, but they could also stem from insider threats, such as disgruntled employees or vendors. Sometimes, an insider threat may even collaborate with an external cybercriminal in exchange for payment by giving them the information needed (e.g., the target's personal details or the company's MFA requirements) to move forward with a SIM-swapping attack. Any employee could be vulnerable to a SIM-swapping attack, but cybercriminals may be more likely to target certain types of individuals, namely executives. These individuals are common targets because they often have a strong online presence, making it easier for cybercriminals to gather their personal information. Furthermore, executives typically have the greatest access to critical company assets and may frequently engage in high-value transactions, thus attracting cybercriminals who are looking to cause widespread damage or steal substantial funds. Regardless of who the target is, it's vital for organizations to ensure all employees are prepared to protect against SIM-swapping attacks.

## Prevention and Response Methods

Organizations can implement several methods to help prevent and respond to SIM-swapping attacks. Here are some best practices for organizations to consider:

- **Ensure sufficient account security measures.** Cybercriminals need users' passwords before they can deploy SIM-swapping attacks and exploit MFA. By requiring employees to create complex and unique passwords that are difficult to crack and change on a regular basis, organizations can stop cybercriminals in their tracks. Additional account security measures that can help minimize SIM-swapping attacks include setting up account activity alerts, utilizing strict access controls and leveraging a virtual private network.
- **Leverage alternative MFA options.** Because SIM-swapping attacks often rely on MFA-related requests being sent via text, organizations should explore other account verification options that cybercriminals can't access through a stolen mobile profile. Potential MFA alternatives include biometrics (i.e., face or fingerprint scanning), physical security tokens or standalone authentication applications.
- **Protect personal details.** Organizations should encourage employees to protect their personal details by keeping their social media accounts private and refraining from sharing this information over text or email, especially to unknown or suspicious recipients. This can make it harder for cybercriminals to obtain the information needed to trick mobile carriers into conducting a SIM swap.
- **Consult mobile carriers.** As SIM-swapping attacks become more common, some mobile carriers have developed measures to help protect against them, such as requiring users to disclose a personal identification number or answer extra security questions before they can make profile changes or transfer cellphone services to different devices. With this in mind, organizations should discuss these security offerings with their mobile carriers and follow any other guidance provided by their carriers to reduce the risk of SIM-swapping attacks.
- **Educate employees.** Organizations should train their employees on SIM-swapping attacks, detecting them and related incident reporting protocols. Key signs of these attacks that employees should be aware of include unanticipated mobile service outages, glitches or disruptions; suspicious account notifications; sudden account restrictions; and unauthorized network activities or transactions.
- **Have a plan.** Creating cyber incident response plans can help organizations ensure necessary procedures are taken when cyberattacks occur, thus keeping related damages to a minimum. These plans should be well-documented and practiced regularly, and they should address a range of cyberattack scenarios (including SIM-swapping incidents). Specific response measures for employers to consider when planning for SIM-swapping attacks include contacting the affected user's mobile carrier, reaching out to financial institutions to temporarily freeze accounts and prevent the theft of company funds, and reporting the incident to relevant authorities.
- **Secure ample coverage.** Finally, employers should purchase adequate insurance to maintain much-needed financial protection against losses that may arise from SIM-swapping incidents. It's best for organizations to consult insurance professionals to discuss their particular coverage needs.

## Conclusion

With SIM-swapping attacks on the rise, it's crucial for organizations to fully comprehend these incidents and take proper steps to protect against them. In doing so, organizations can equip themselves with the knowledge and resources to mitigate related cyber losses and successfully navigate today's evolving digital threat landscape. Contact us today for more risk management guidance and insurance solutions.