



How SIM Swaps Bypass Your Online Security

How SIM Swaps Bypass Your Online Security

Have you ever been in the middle of an important phone call or task on your phone when you suddenly see those dreaded words, "SOS only" or "No Signal"?

Most of the time, it's simply due to poor signal strength in your area or a temporary glitch with your carrier's network. But what if losing your phone connection wasn't so innocent?

What if an unknown hacker actively removes you from your mobile number to take it over for their own malicious purposes? This is the frightening reality of a cybercrime called "SIM swapping," and it's a growing threat that has affected many unwitting victims.

How Hackers Carry Out SIM Swapping

Hackers gather personal information, such as your name, date of birth, and address, through data breaches or social engineering. They then contact your mobile carrier with enough information about you to answer the verification questions. They

impersonate you and claim to have lost your SIM card.

Mobile network carriers that don't sufficiently verify customers often make it possible for a hacker to convince an employee to port your phone number to a new SIM card under their control.

This is done without triggering notifications to your devices or email addresses. Within minutes, you could find yourself disconnected from your mobile number while the hacker now receives all calls and texts intended for you. The whole process can be carried out remotely.

The Risks of Losing Access to Two-Factor Authentication

Once hackers control your phone number, they can bypass the two-factor authentication that protects many of your online accounts. Most major services send one-time verification codes via text when you attempt to log in from a new device. With your SIM swapped, these codes get diverted to the hacker.

This can then allow the hacker access to your emails, finances, cryptocurrency,

and any other service that uses SMS-based two-factor authentication.

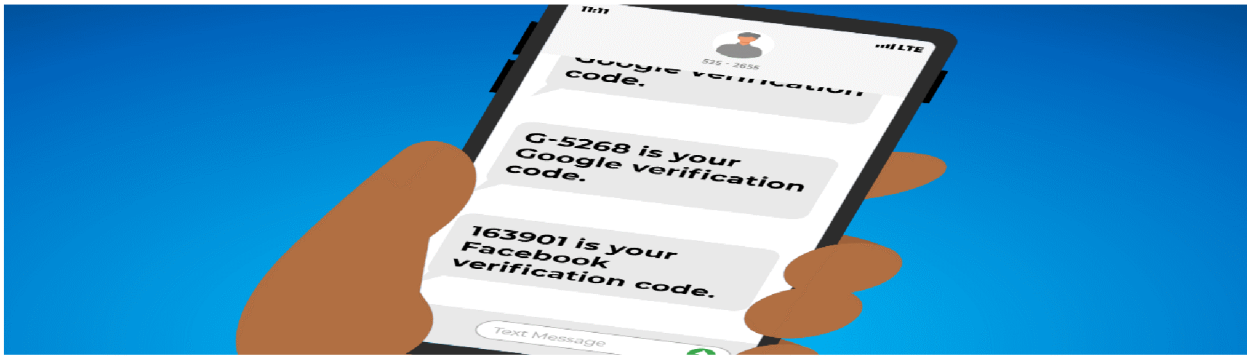
To make matters worse, restoring access to your accounts becomes a nightmare without your phone number.

Preventing SIM Swapping Attacks

- Do not share personal details unnecessarily online or over the phone. Be wary of attempts at social engineering.
- Limit what information you make publicly available on social media profiles or in public records.
- Use authentication apps such as Google Authenticator or Authy instead of SMS-based codes wherever possible.
- Contact your mobile carrier and ask them to put a PIN or passcode on your account as an extra security step before any changes can be made.

By taking these steps, you can help protect yourself from having your phone number and online accounts compromised by SIM swapping.

Staying vigilant about cybersecurity is important for everyone in the digital age.



Unexpected 2FA Codes: Your Cybersecurity Wake-Up Call

Unexpected 2FA Codes: Your Cybersecurity Wake-Up Call

We've all had those moments of confusion when our phone buzzes with a notification that doesn't seem quite right. If you've ever woken up to a text with some random numbers and wondered what it is, you're not alone.

Getting a code for two-factor authentication (2FA) from a service you use when you didn't request one deserves some attention. Rather than ignoring the strange message, it's a good idea to take action to help protect your online accounts.

Understanding 2FA

2FA, or "Two-Factor Authentication," is an important security feature many apps and websites use. It adds an extra verification step beyond just a password. After you log in, 2FA will text or email you a special code to enter before you're given access to your account. This acts like a second lock, keeping hackers out even if they somehow steal your password.

Spot the Warning Signs

When you receive a 2FA code you didn't request, it's a clear sign that someone is trying to access one of your online accounts. It often indicates that your password has been compromised through a large-scale data breach or a more targeted attack. Hackers may be

attempting to log in using your stolen credentials, and the 2FA code is the only thing standing in their way.

Taking Immediate Action

Rather than ignoring the 2FA code or brushing it off, it's important to act right away to secure your accounts.

- Do not click on any links in the email or SMS. Open a browser, log in to the relevant account, and change your password to something unique and complex. Make sure it's different from the one you used before and not used for other accounts.
- Check if your old password was involved in any known breaches using a tool such as [HaveIBeenPwned.com](https://haveibeenpwned.com). This can help you identify if you have any other accounts that may be at risk.
- Consider changing passwords for any other accounts using the same or similar passwords in case of credential stuffing attacks. This is when hackers use stolen passwords from one breach to try and access other accounts.
- Be wary of emails or texts asking you to provide a 2FA code. Legitimate services will

never ask for this, and it's likely a phishing attempt.

This unexpected 2FA code experience is a valuable reminder of the importance of proactive security measures. Two-factor authentication is what saved you this time by blocking the hacker's attempt to access your account, so take a moment to ensure you've enabled it on every site that offers it.

Additionally, using unique, strong passwords for each account is essential to prevent the ripple effects of a single data breach. A password manager can help you generate and store complex credentials, ensuring one compromised password doesn't put all your other accounts at risk.

While complete online security can never be guaranteed, taking these fundamental steps – enabling 2FA and using unique passwords – goes a long way toward safeguarding your personal information and digital identity.

Contact us today at 940-282-0290 if you would like more information pertaining to SIM swaps and Two-Factor Authentication (2FA).

We are here to help you become more secure in today's digital age.