



SIM Swapping

Recovering from SIM Swap or Port-Out Fraud

SIM swapping (also called SIM hijacking or SIM port-out fraud) occurs when criminals convince or trick a mobile carrier into transferring your phone number to a SIM card they control. Once successful, the criminal receives your calls and text messages, often including one-time passcodes used to reset passwords and access accounts.

SIM swapping is especially dangerous because many services rely on text messages to verify identity. When your number is hijacked, criminals may quickly take over:

- Email accounts
- Banking and financial accounts
- Social media
- Cryptocurrency wallets
- Work or school systems

If you suspect SIM swapping, act quickly. Minutes matter.

Signs You May Be a Victim of SIM Swapping:

- Sudden loss of cell service (“No Service” or “SOS Only”)
- Calls and texts stop working unexpectedly
- You receive alerts about account changes you didn’t make
- Password reset notifications you didn’t request
- Accounts become inaccessible shortly after phone service loss
- Carrier notifies you of a SIM or port change you didn’t authorize

SIM Swapping – Do This First

Act Quickly

- Treat this as an incident requiring urgent account-recovery response
- Do not wait to see if service returns
- Assume criminals are actively attempting account takeovers

Contact Your Mobile Carrier

- Use another phone (friend, family, or landline).
- Tell them clearly:
 - “I believe I am the victim of SIM swap fraud. My number has been transferred without authorization.”
- Ask the carrier to:
 - Suspend the compromised SIM
 - Restore your number to a secure SIM





- Lock the account against further port-outs
 - Add or verify a PIN / passcode on the account
 - Review recent changes and document the incident
- Request a case or incident number.

Secure Financial & Critical Accounts (From a Safe Device)

Once your number is secured or if possible in parallel:

- Contact banks, credit cards, and payment apps immediately
- Inform them of SIM swap fraud
- Freeze or monitor accounts as advised
- Change passwords for:
 - Email
 - Financial accounts
 - Social media
 - Work or school systems
- Remove phone number-based recovery where possible

Replace SMS-based recovery with passkeys, authenticator apps, or security keys where supported.

Preserve Evidence

Before deleting alerts or messages:

- Screenshot:
 - Carrier notifications
 - Account takeover alerts
 - Password reset messages
- Record:
 - Date and time service was lost
 - Carrier interactions
 - Any financial loss or attempted transfers

This documentation is critical for recovery and reporting.

Report the Crime

SIM swapping is a recognized form of identity theft and fraud.

- National Reporting
 - If the carrier mishandles the SIM-swap or port-out response, file a complaint with the FCC Consumer Complaint Center.
 - FBI Internet Crime Complaint Center (IC3)
<https://www.ic3.gov>
- Ohio Resources
 - Ohio Attorney General – Identity Theft & Cybercrime Help
<https://www.ohioattorneygeneral.gov>
Hotline: 800-282-0515





- Geauga County
 - Geauga County Sheriff's Office
<https://www.geaugasheriff.org>
 - Local police non-emergency line if fraud or threats occurred

Law enforcement can:

- Document identity theft
- Support financial recovery
- Coordinate with federal agencies

Recovery – After Your Number Is Restored

- Monitor all accounts closely for several weeks
- Review bank and credit statements daily
- Confirm carrier account notes and protections are active
- Notify employers or schools if your number was used for access
- Consider placing a fraud alert or credit freeze if identity data was exposed

How to Reduce the Risk of SIM Swapping

- Treat your phone number as a high-value identity asset
- Be cautious about sharing your number publicly
- Verify unexpected messages or calls claiming to be from your carrier
- Act quickly if service is lost without explanation
- Ask for help early, delays increase damage

