

What is a SIM Swapping Scam? Protect Your Device Against SIM Hackers

Archived: 2026-04-05 21:21:14 UTC

Stay a step ahead of the scammers. Educate yourself on some of the most common frauds and scams.

I need to report an unauthorized SIM change.

If you received a message from Verizon advising that a new SIM card or a new device is being activated on your line and you or an Account Manager on your account did not make this request, contact us immediately by dialing *611. This is an airtime-free call and will work even if your device has been deactivated. You can also call us by dialing 1-800-922-0204 from any phone. If you need to contact us after regular business hours, [Chat With Us](#) and, after logging in, type 'Live Agent' into Verizon Chat Assistant to access 24 hour live chat support.

What is an unauthorized SIM change, also known as a SIM swap?

Unauthorized SIM changes, sometimes called SIM swapping or SIM hijacking attacks, occur when a customer's phone number is transferred to a different SIM card or eSIM profile under the control of a criminal. If the SIM swap is successful, the criminal may intercept the customer's phone calls and text messages to receive one-time security codes from social media, banks, credit card companies, cryptocurrency exchanges, and other financial institutions, allowing them to potentially access those accounts and cause financial and reputational harm to the customer.

But, not all SIM changes are bad! Authorized SIM swaps may happen when you upgrade your device, or when you troubleshoot or replace a lost or stolen device.

How does fraudulent SIM swapping work?

Criminals typically use SIM swaps as a way to steal your phone number so they can access your bank or other financial accounts. They often start by gathering as much personal information about you as they can from social media, the Internet, the dark web, previously compromised accounts, and directly through [phishing](#)¹. They use this information to pretend they are you, in an effort to gain access to your Verizon account and transfer your mobile number to a different SIM card or eSIM under their control. Once they've "swapped" your SIM, calls and texts to your phone number route to the phone in the criminal's control. At that point, the criminals can use their phone to receive one-time security codes or calls that banks and other companies use to safeguard customer accounts. In some cases, you might not know this has even happened until your phone no longer works.

1. Phishing

Phishing occurs when criminals send you fraudulent requests for personal information, usually posing as a company or government agency.

How to protect against SIM swap.

Protect your account by following these best practices:

1. **Add SIM Protection** At no cost to you, SIM Protection offers you the ability to lock lines on your account to prohibit changes to the SIM cards associated with those lines. No request to change your SIM will be processed until you unlock the SIM protection feature on the line. See instructions below on how to add SIM Protection.
2. **Use strong and unique passwords.** Each of your online accounts should have a strong and unique password or passphrase. Resist the temptation to reuse passwords or create similar passwords across various accounts, especially between social media and financial accounts. Always enable two-factor authentication wherever it's available. Use a password manager to create and manage complex passwords.
3. **Be suspicious of unsolicited texts, e-mails, and calls, especially those urging you to act immediately and provide personal details.** Verizon will **never** contact you to request any password, PIN, social security number, or payment information. If you receive a suspicious text message claiming to be from Verizon, please forward it to us right away at S-P-A-M (7726), then delete it. Also, don't ever share your personal information online, and never reply to calls, emails or text messages that ask for personal information.
4. **Give your online security an upgrade.** If you have been the victim of a SIM hijacking attempt, you should change the passwords for services such as your financial institutions and e-mail immediately. Use the "security dashboard" of your e-mail provider to look for any suspicious logins from computers or locations you don't know. Change your passwords on a regular basis and review your credit report often to check for any unauthorized accounts or inquiries. [Review Verizon's tips for preventing phishing attacks.](#)

How do I add SIM Protection?

At no cost to you, SIM Protection offers you the ability to lock the lines on your account to prohibit changes to the SIM cards associated with those lines.

Only authorized Account Owners or Account Managers can enable or disable SIM Protection for all lines on the account.

- **Verizon Wireless postpaid customers:** This feature is available through the [My Verizon website](#)² and [My Verizon app](#).³

3. My Verizon App.

To enable/disable SIM Protection through My Verizon app: for Postpaid

Sign in to My Verizon.

1. Select Account Tab at the bottom of the screen.
2. Select Edit Profile and Settings (Under Welcome and Your Name).
3. Scroll to the Security Menu.
4. Select SIM Protection.

5. Select the appropriate number(s) to protect (i.e., by toggling On or Off).

- If SIM Protection is on, green displays on the toggle button.
- If SIM Protection is off, black displays on the toggle button.

Lines that have SIM Protection enabled are blocked from all transactions requiring a new SIM, including SIM swaps, device upgrades, and bring-your-own-device transactions.

When SIM Protection is turned off, there is a 15-minute delay period before transactions requiring a new SIM can be completed

2. My Verizon website

To enable/disable SIM Protection through My Verizon website for postpaid customers

1. Sign in to My Verizon.
2. Select Edit Profile and Settings (Under Welcome and Your Name).
3. Scroll to the Security Menu.
4. Select SIM Protection.
5. Select the appropriate number(s) to protect (i.e., by toggling On or Off).

- If SIM Protection is on, green displays on the toggle button.
- If SIM Protection is off, black displays on the toggle button.

Lines that have SIM Protection enabled are blocked from all transactions requiring a new SIM, including SIM swaps, device upgrades, and bring-your-own-device transactions.

When SIM Protection is turned off, there is a 15-minute delay period before transactions requiring a new SIM can be completed.

- **Verizon Wireless prepaid customers:** This feature is available through the [My Verizon website](#)⁴ and [My Verizon app](#)⁵.

5. My Verizon App

To enable/disable SIM Protection through My Verizon App for prepaid

1. Sign in to My Verizon.
2. Click the menu icon in the upper left corner.
3. Select Account.
4. Select Account Settings.
5. Click on the Security tab.
6. Select Manage SIM Protection.
7. Select the appropriate number(s) to protect (i.e., by toggling On or Off).

- If SIM Protection is on, green displays on the toggle button.
- If SIM Protection is off, black displays on the toggle button.

Lines that have SIM Protection enabled are blocked from all transactions requiring a new SIM, including SIM swaps, device upgrades, and bring-your-own-device transactions.

When SIM Protection is turned off, there is a 15-minute delay period before transactions requiring a new SIM can be completed.

4. My Verizon Website

To enable/disable SIM Protection through My Verizon website for prepaid

1. Sign in to My Verizon.
 2. Go to Account > Account Overview > Settings.
 3. Under Manage Account Settings, scroll down and click on SIM Protection.
 4. On the SIM Protection page, select the appropriate number(s) to protect (i.e., by toggling On or Off).
- If SIM Protection is on, green displays on the toggle button.
 - If SIM Protection is off, black displays on the toggle button.

Lines that have SIM Protection enabled are blocked from all transactions requiring a new SIM, including SIM swaps, device upgrades, and bring-your-own-device transactions.

When SIM Protection is turned off, there is a 15-minute delay period before transactions requiring a new SIM can be completed.

- **Verizon Wireless Business customers:** This feature is available through the [My Business](#) application or webpage and My Business Application (Find out how on the [My Business Support](#) page).

When SIM Protection is enabled on a line, the status of the line is changed to Locked. A Locked line cannot process a SIM change and device upgrade until the SIM Protection is turned off. This ensures that your number is protected from SIM swapping.

When SIM Protection is added, you will receive a notification via a text message that the feature is turned on and active.

How do I remove SIM Protection?

Disable SIM Protection

When you need to request a SIM change or device upgrade on your line, you can simply turn the SIM Protection off in the same menu where you turned it on. When you change the SIM Protection status to Unlocked, it will take 15 minutes before the restrictions are lifted. After 15 minutes, you will be able to make any needed SIM changes or submit device upgrade orders for your line. Please note that, for account security, our retail and customer service representatives are not able to turn SIM Protection off for you - it must be disabled through the My Verizon website or the My Verizon app.

When SIM protection is turned off, you will receive a notification via SMS that the feature has been turned off.

To prevent unauthorized users from taking control of your line, we encourage you to turn the SIM Protection back on as soon as you complete the SIM change or device upgrade.

Source: <https://www.verizon.com/about/account-security/sim-swapping>