SIM SWAPS and other ACCOUNT TAKEOVERS:
Keeping your accounts secure

What is a SIM card?

A SIM card is a small chip in your cell phone that has a unique number which your cell phone service provider (AT&T, Verizon, T-Mobile, Sprint) associates with your account. The service provider routes calls and texts directed to your phone number to the SIM card identified in your account records, which *should* be the SIM card inside your cell phone. If the SIM card number linked to your phone number changes, calls and texts to your phone number will be received by whatever phone contains that new SIM card.

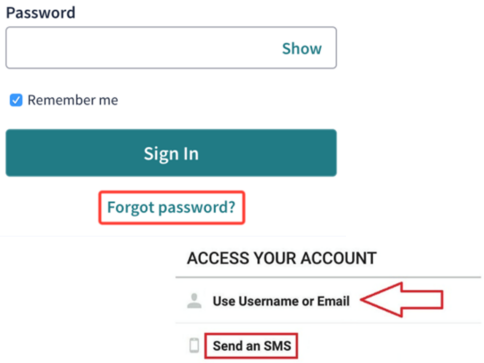
What is a "SIM swap"?

An unauthorized "SIM swap" happens when malicious actors cause your cell service provider to alter your account records, changing the SIM card number assigned to your phone number from the SIM card in *your* phone to one in *their* phone. There are various ways to accomplish this, and it is extremely difficult to prevent. Once the swap is complete, the rogue device receives any calls or texts sent to your phone number.

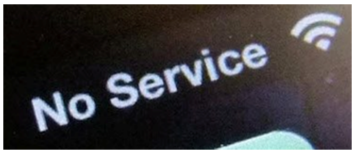
How can this hurt me?

Once they control your phone number, hackers visit the login pages for online accounts linked to that phone number (email, social media, financial and cryptocurrency accounts, communication accounts, accounts used for two-factor authentication, etc.) and request the sending of "password reset" codes to the phone number linked to the account. If they receive the code, they use it to reset the password on the account, thereby gaining access to your account and taking over control of it.

If the newly compromised account is linked to other accounts, the hackers may be able to receive password reset codes sent to the compromised account to reset passwords in those linked accounts, and so on.



How will I know if I get SIM swapped?



Unexplained loss of cell service is the first sign that a SIM swap is happening. If your phone is connected to WiFi, you may start receiving emails or other notifications of actual or attempted logins from new devices, or actual or attempted password resets on some of your accounts.

What can I do if it happens to me?

1. Regain control of your phone number. The longer they control your number, the more damage they can do. Call your cell service provider's fraud department or visit a store. Be prepared to verify your identity, but regardless, the agent should be able to see a new device is being used and suspend service pending further investigation.
2. If any other account (email, etc.) is taken over as a result, reset the password yourself (if you can) to regain access, and terminate all other active sessions to kick out the hacker(s). If you can't get back in yourself, report it immediately to the company (perhaps via phone call, customer support chat, or support ticket). Ask them to terminate any active sessions and freeze the account until you can prove you are the authorized account holder.
3. If any communication account was taken over (Twitter, Telegram, Instagram...), consider that the hackers may have reached out to your contacts while pretending to be you. You may need to take corrective action.

Can I prevent my phone number from being SIM swapped?

Probably not—for the most part this is out of your control. Setting up a PIN number or other form of enhanced authentication with your phone service provider can't hurt, but ultimately it probably will not prevent this type of attack. Your best protection is to ***manage how you handle account recovery and two-factor authentication ("2FA")*** to prevent hackers from using those processes against you (see page 2).

SIM SWAPS and other ACCOUNT TAKEOVERS:
Keeping your accounts secure

[cont'd from page 1] What can I do to protect myself?

Assume a SIM swap or password compromise is going to happen, and manage your online security so that there is little the hackers can do as a result. In managing any account accessible via the Internet, consider the following:

- **Start with an email account that can be (and is) secured with a HARDWARE TOKEN *(see below)***. Remove your phone number from that account entirely. Secure your alternate email the same way (hardware token, no phone number). Use this secure email as your contact/login for all your online accounts, and for two-factor authentication ("2FA") or account recovery whenever a better method is not available (see below).
- **Separate your phone number from your online accounts**. NEVER use your phone number (SMS or voice calls) for 2FA. Remove your phone number as an option for account recovery. Remove it entirely whenever feasible, to prevent it being used as a means to verify identity. If an account forces you to link a phone number, use an anonymous prepaid service or VoIP number (such as Google Voice) that you do not use for everyday contact.
- **Use secure two-factor authentication ("2FA") whenever possible**. Hardware token is best. Software 2FA apps (Google Authenticator, Microsoft Authenticator, Authy) are safe only if backup/recovery codes are only stored in a secure place, AND if you restrict the adding of new devices (which is often enabled by default) to prevent a hacker from using your compromised phone number to duplicate your authenticator app on a new device.
- **Change answers to "challenge questions" to something fictitious** so they can't be guessed (but keep track!).
- **Digital storage of passwords or private keys should ONLY be in a secure PASSWORD MANAGER *(see below)***.

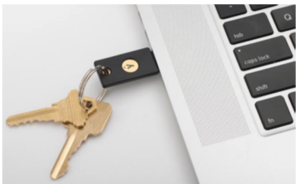
A PRACTICAL APPROACH TO ACCOUNT SECURITY:
Hardware Token + Password Manager

The best way to protect your accounts—against SIM swaps, password leaks, and a variety of other attacks—is to use strong, unique passwords for every account, and assume that those passwords can and will be compromised. One practical way to accomplish this is to store passwords (and other sensitive information) in a high-quality password manager application, and use a hardware token to secure that password manager and any other account used for authentication or account recovery.

Hardware Tokens (aka Hardware Keys)

Hardware tokens (Yubikey and Thetis, shown below, are popular examples) provide secure 2FA by enabling the user to generate one-time passwords for account access without ever exposing the private key or needing to protect a shared secret between the user and the service provider. The code for account access can only be generated by someone with physical possession of the token-generating device. TIPS FOR USE:

- Keep a backup—register at least 2 token devices on each account you use them on; keep one with you, and the other in a secure location.
- Make sure the product you choose is compatible with the devices and services you use.



Password Managers

Password managers provide a convenient way to use strong, unique passwords for every account, without having to remember them or risk storing them somewhere unsafe. They can store (and auto-fill) logins and passwords for all your accounts, as well as other information used for authentication (such as answers to challenge questions). They can also auto-generate strong passwords so you are not limited by your own creativity. TIPS FOR USE:

- Pay for a good one—they are inexpensive and well worth it for the security and convenience provided.
- Secure it with a hardware token and take all the other security precautions described above to protect it from compromise.

Dashlane LastPass 1Password