HOW TO PROTECT YOURSELF FROM
SIM SWAP SCAMS

SIM swapping is a malicious technique where criminals target mobile carriers to steal access to victims' bank accounts, virtual currency accounts, and other sensitive information. They do this by tricking mobile carriers through impersonation, or using phishing tactics attempting to switch a victim's mobile number to a SIM card in the criminal's possession.

HOW DO SIM SWAP SCAMS WORK?

1. Scammer calls your cell phone service provider, pretends to be you, and says your phone was lost or damaged.

2. Scammer asks the service provider to activate a new SIM card for your phone number on a new device they own.

3. Service provider activates the new SIM card. The scammer—not you—will get all your text messages, calls, and data on the new phone.

4. Scammer logs in to your accounts that use texts as a form of MFA, since they now get texts with the verification code needed to log in.

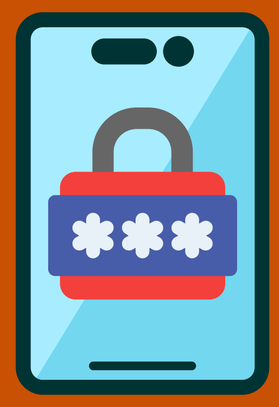
HOW CAN YOU PREVENT THEM?

Don’t reply to calls, emails, or texts requesting personal information.

These could be phishing attempts by scammers looking to get personal information to access your cellular, bank, credit, or other accounts.

Set up a PIN or password on your cellular account.

This could help protect your account from unauthorized changes. Check your cell phone provider’s website for information on how to do this.



Limit the personal information you share online.

Avoid posting your full name, address, or phone number on public sites. Anyone can find that information and use it to answer security questions required to verify your identity and log in to your accounts.

Consider using stronger authentication on accounts.

If you're concerned about SIM card swapping, use an authentication app or a security key for accounts containing any sensitive personal or financial information.

Have questions? Contact us at infosec@miami.edu