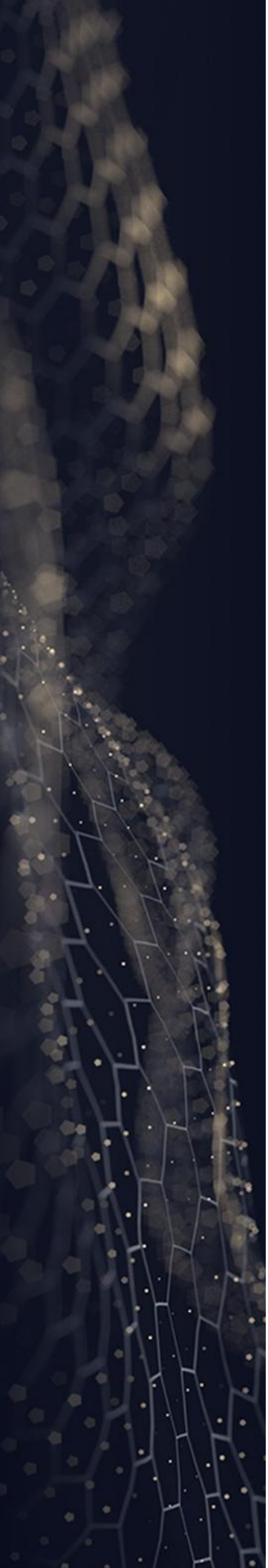
Wireless Carrier Security

Client Guide



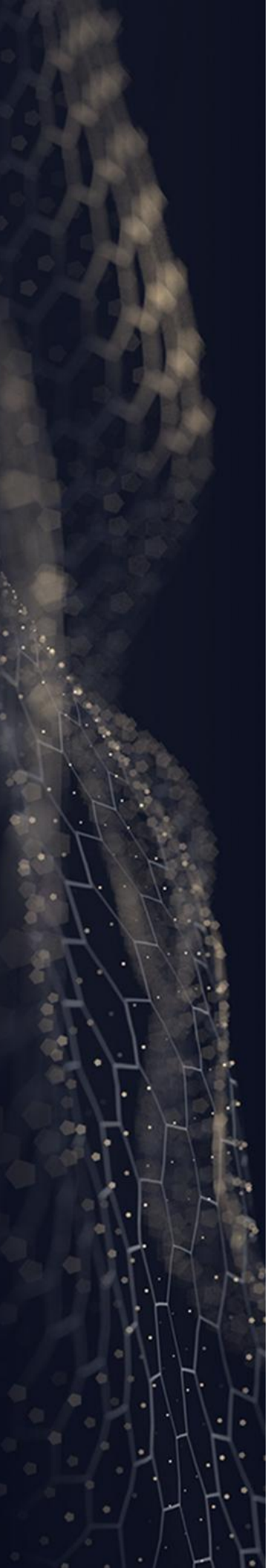
This document will serve as a guide for enhancing cell phone security at the account level for the 4 major wireless carriers: Verizon, AT&T, T-Mobile & Sprint. Across all for 4 major carriers, we recommend implementing these enhanced security measures:

- **Setting a PIN at the account level.**
  - Adding a PIN or passcode to your account, adds an extra layer of security. In order to make changes to your account, this PIN is required. Some carriers set the PIN as the last 4 digits of the primary account holder's SSN, so be sure to change this code to something unique. Consider updating the PIN periodically.

- **Enabling Two-Factor Authentication (2FA) (if available by the carrier)**
  - To further protect your account beyond your username and password, setting up 2FA will require an additional authentication factor like an SMS text message sent to your phone, a code delivered to your email or a code generated via an authenticator app like Google Authenticator or Authy.
  - If 2FA is unavailable, we recommend setting Security Questions and a PIN for your account.

- **Using a strong password and update it periodically**
  - We recommend 14 characters or longer, using upper and lower case, and a mixture of numbers, letters and special characters.

- **Keep your personal information and passwords private**
  - Don't share account information, PIN or passwords.



The 4 major carriers implement slightly different safeguards for protecting customer accounts. Here are specific features available at Verizon & T-Mobile that we've found.

VERIZON

- **Number Locking**
  - Number locking prevents an unauthorized port out or SIM Swap of your mobile number. You must select which phone numbers associated with your account that you want to lock.

T-MOBILE

- **Port Validation**
  - In addition to your account PIN, you can also set a 6-15 Digit passcode that will be added to your account to restrict port changes.

- **Biometric Verification**
  - Allows you to verify your account by your T-Mobile ID when you call into Customer Care for assistance using the T-Mobile app and biometric credentials such as Face ID or fingerprint recognition, so you don't have to remember your PIN or Passcode.

- **NOPORT**
  - NOPORT adds another layer of security on top of T-Mobile's Port Validation but it's not known if that's a feature that every customer can enable, and if not, which customers can get it. If you've experienced fraud on your wireless account, you will likely be able to obtain this feature. When NOPORT is enabled on your account, T-Mobile requires a customer to visit a retail store and present a government-issued photo ID in order to have their number ported to a different carrier or get a new
    SIM card.

The next few pages will outline the exact steps you should take to implement security features at each of the specific carriers.

ACCOUNT IMPLEMENTATION

VERIZON WEB:

- **Set Up A PIN**
  - Navigate to Wireless account page > Change Account Pin Page
  - Sign in to the account
  - Enter the new account PIN, then re-type in designated box
  - Click submit to confirm

- **Set Up Two Factor Authentication**
  - Navigate to Wireless account page >
  - Sign in to the account.
  - Select upper right Menu > Account
  - Navigate to the Two-factor authentication section and turn ON, "Enable two-factor authentication"
  - Save Changes

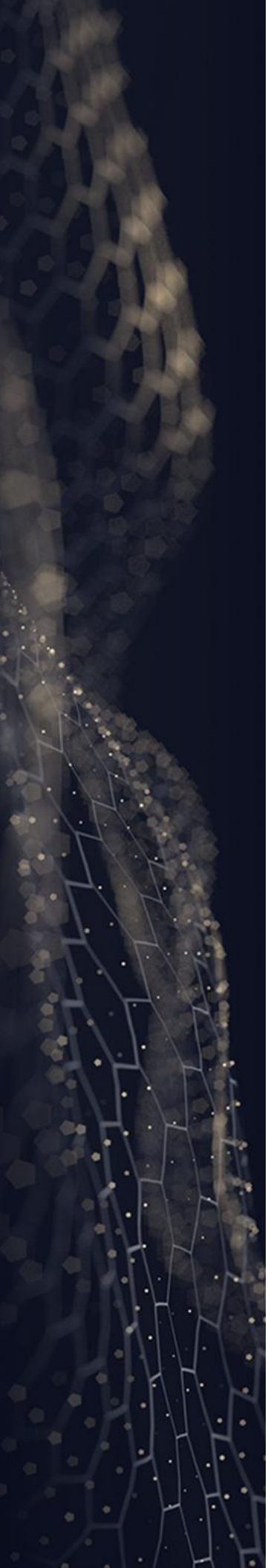
- **Number Locking**
  - Navigate to Wireless account page >
  - Sign in to the account.
  - Select upper right Menu > Account

- Navigate to the Number Lock section and turn ON for each mobile device you want to Lock.
- Save Changes

AT&T WEB:

- **Set Up A PIN** (*All customer accounts are created with a PIN/Passcode during their initial account setup. The default is the last 4 of the account holder's SSN, so we recommend changing that immediately upon account creation. If you've never updated your PIN/Passcode follow the steps below to update it*)
  - Navigate to Wireless account page > My Account > User Profiles > Select Edit under Primary Account
  - Sign in to the account
  - Enter the new account PIN, then re-type in designated box
  - Click submit to confirm
  - Scroll down to Security System access codes
  - Select Edit PIN
  - Enter new PIN
  - Repeat > Save

- **Set Up Two Factor Authentication**
  - Two Factor Authentication on wireless accounts is enabled by default and cannot be turned off.



T-Mobile

T-MOBILE WEB:

- **Set Up A PIN** (*If you have not established a PIN for your account upon logging in you will be prompted to do so*)
  - Sign in to My T-Mobile account
  - Choose a verification method, either SMS / Security questions
  - Select Next > Follow prompts for signing with this method
  - Navigate to Set Your PIN/Passcode > Enter desired PIN/Passcode > Next/Save

- **Setting 2 Step Verification**
  - Sign in to My T-Mobile account
  - Profile > T-Mobile ID > Enable 2-Step Verification, preferably with an authenticator app

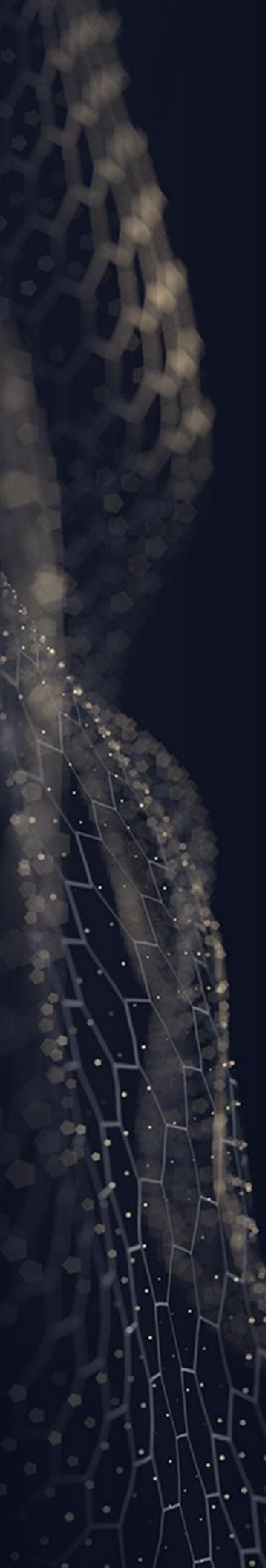
T-MOBILE CUSTOMER SERVICE

(call 611 from your T-Mobile phone or dial 1-800-937-8997 from any phone):

- **Port Validation**
  - Request to add Port Validation and create a 6-15 digit code over the phone with the Customer Care representative

- **Set Up Biometric Verification**
  - There are some qualifications and additional steps to take to enable this feature here is the link with those details:
    - Set up biometric verification

- **Request NOPORT**
  - The Primary Account Holder must call T-Mobile Customer Service to Enable this



SPRINT WEB:

- **Set Up A PIN and Security Questions** (*Sprint requires all customers to create a PIN during their initial account setup*)
  - Sign in to sprint.com
  - Select My Sprint (or My Account) > Profile & Security (or Profile & Settings)
  - Scroll down to Security Information
  - Update PIN or security question/answer and save it

NEED ASSISTANCE?

Email us at ask@blackcloak.io and we'll answer any questions you have and assist you in any of the processes described above.