Consumer Guide

Protecting Your Personal Data

Our mobile phones know a lot about us and the data generated by our devices is increasingly being used in unexpected ways. Geolocation and other data, such as who we call, is sensitive and personal. With data breaches increasing in frequency and severity, it's important to take steps to safeguard your data.

Data Protected by FCC Rules

FCC rules protect customer proprietary network information (CPNI) in the carriers' possession. This information includes: the location of an active mobile device; the phone numbers called by a consumer; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting.

Under the Telecommunications Act, carriers must protect the privacy and security of their customers' service-related and billing information, and may only use, disclose, or permit access to CPNI under these conditions:

- As required by law.
- With customer approval.
- While providing the service for which the customer information was obtained.
- When providing a 911 caller's location information to a 911 call center.

If you believe your carrier or provider is selling or sharing your location or other CPNI protected information, you can file privacy complaint with the FCC online, by visiting https://consumercomplaints.fcc.gov; or call 1-888-CALL-FCC (1-888-225-5322); ASL: 1-844-432-2275.

The FCC requires telecommunications carriers and interconnected Voice over Internet Protocol (VoIP) providers to notify customers and federal law enforcement of breaches that expose CPNI data. Carriers are also required to submit to the FCC an annual summary of all consumer complaints received regarding unauthorized release of customer information and certify it is compliant with FCC rules.

For more information check the FCC Consumer Guide: Protecting Your Privacy: Phone and Cable Records.

Take Steps to Protect Your Data

Creating a strong password is an essential step to protecting yourself online. Using long and complex passwords is one of the easiest ways to defend yourself from cybercrime and to protect your data online.

- Make passwords hard to guess. Do not include personal information in your password, such as your name or pets' names, birth dates, or favorite sports teams. These can easily be found on social media.

- Avoid using common words in your passwords.
- Keep your passwords a secret. Don't tell anyone your passwords and watch for attackers trying to trick you into revealing your passwords through email or calls.
- Unique account, unique password. Having different passwords for various accounts helps prevent cyber criminals from gaining access to these accounts and can protect you in the event of a breach.
- Double your login protection. Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in.
- Use a password manager to remember all your long passwords. The most secure way to store all of your unique passwords is by using a password manager. The Cybersecurity and Infrastructure Security Agency and the National Cybersecurity Alliance have partnered to provide SIMPLE TIPS for creating a password.

Think before you connect to Wi-Fi networks and Bluetooth. Unsecure connections may compromise sensitive information stored on your device and in online accounts. Take these steps to minimize the risk:

- If you regularly use a public Wi-Fi hotspot, consider using a virtual private network (VPN) that will encrypt your data.
- Adjust your device's settings so it does not automatically connect to nearby Wi-Fi networks.
- Websites that are secure use "https" at the beginning of their web address. If the "s" is missing, avoid sharing any sensitive data or information.
- When sending sensitive information, your mobile data plan may be more secure than Wi-Fi.
- Turn Bluetooth off when not in use. Use Bluetooth in "hidden" mode rather than "discoverable" mode. This prevents other unknown devices from finding your Bluetooth connection.
- If you connect your mobile phone to a rental car, be sure to unpair your phone and clear any personal data from the car before you return it. Take the same steps when selling a car.
- Check out FCC Consumer Guide: Wireless Connections and Bluetooth Security Tips.

Additional Consumer Guides to Help Protect Your Information

- Cell Phone Fraud
- Mobile Wallet Services Protection
- Stop Unwanted Robocalls and Texts
- Caller ID Spoofing