City & Police
FEDERAL CREDIT UNION

SECURITY TIPS FOR BANKING ON THE GO

Best Practices

Lock Your Phone – Secure your mobile device with a password. If your mobile device is ever lost or stolen, it will protect your private and secure information.

Texting or Email – Use caution with your private information. Don't text or email confidential information about your account to anyone.

Identity Protection – Don't respond to a "phishing" text or email that requests your PIN, account number or any card information, and please remember that City & Police will never request information in this manner.

Opening Files – Be wary of unsolicited files, text messages or applications, especially if they are received from unknown sources.

Application Downloads – Only download and install applications from reliable sources and report any banking application that appears to be malicious to City & Police right away.

Secure Websites – Look for security symbols such as an icon of a lock or an "https" in the URL.

Connection & Log Out – Only connect to financial accounts via a secure connection or a non-public Wi-Fi network, and remember to log out of Mobile Web and Mobile Apps when you are finished with your session.

Bluetooth – Consider disabling Bluetooth, or set the Bluetooth status to hidden, until you want to share something.

Monitor – Monitor your accounts on a regular basis to detect unauthorized activity.

Clear It - Be sure to clear out all information from your mobile device before discarding.