Banking in Public
Safety tips to protect your financial information

Whether you're on vacation or taking a trip to the grocery store, the convenience of mobile banking is undeniable. With just a few taps on your smartphone, you can check your balance, transfer funds, pay bills, deposit checks, and more. However, this convenience can come with security risks, especially when banking in public places or using public Wi-Fi networks. Understanding these risks and taking the correct steps — like the tips below — are critical to protect your financial and personal information.

1 Use secure networks

Always use a secure, private network when accessing your online banking accounts. Public Wi-Fi networks are often unencrypted, making it easier for cybercriminals to intercept your data. If you must use public Wi-Fi, consider using a virtual private network (VPN) to encrypt your connection and protect your information from virtual eyes.

2 Create strong, unique passwords or passphrases

Using strong, unique passwords for your online banking accounts is your first line of defense against cyberattacks. Avoid using personal information like birthdays or pet names. Instead, opt for a mix of uppercase and lowercase letters, numbers, special characters, and phrases. Generate a different password for each of your online accounts.

3 Enable two-factor authentification

Two-factor authentication adds an extra layer of security by requiring a second form of verification in addition to your password. This could be a text message code, an email verification, or a biometric authentication like a fingerprint or facial recognition. This extra step will help reduce the risk of unauthorized access to your account.

4 Beware of shoulder surfers

When accessing your online banking in public, be cautious of people around you who might be trying to observe your screen or keyboard inputs. This practice, known as "shoulder surfing," can lead to your sensitive information being stolen. Shield your screen and be discreet when entering passwords or PINs.

5 Log out after each session

Be sure to log out of your online banking account after each session, especially when using a shared or public device. Simply closing the browser or app may not be sufficient, as your session could remain active. Logging out ensures that no one else can access your account if they gain access to the device you were using.

6 Set up account alerts

Many banks offer account alerts that can notify you of various activities, such as card transactions, low balances, password changes, updates to personal information, or failed login attempts. Setting up these alerts can help you stay informed about your account's activities and quickly detect any unauthorized transactions.