**Safe Mobile Banking**

1. **Create a Strong Password**

Use strong passwords to protect your personal information. Passwords should be long — the longer, the better — so hackers have a harder time using code-breaking software to crack it. Strong passwords should contain a mix of letters with capitals and lower cases, numbers, and special symbols. They should not contain any personal information or words you’d find in the dictionary.

Do not use the word “password” or your name and birth year as your login, which is information that hackers can easily find. Also, don’t reuse your passwords. Come up with a new one every time.

### Avoid Using Public WiFi

Do not use public WiFi for mobile banking for it is not secure and that others may be able to watch your online actions. Instead, use your cellular network or your home wi-fi to better protect your personal information. Also, turn off settings on your devices that allow automatic connectivity, which could permit your computer or mobile device to connect to a network that you would otherwise want to avoid. Be sure to monitor your Bluetooth connections as well, since Bluetooth can allow other devices to connect directly to yours.

### Use the Bank’s Official App

United Bank of Philadelphia Mobile Apps:

*For Retail Banking*

 – iPhone

<https://apps.apple.com/us/app/united-bank-of-philadelphia/id1630167752>

– Android phone

<https://play.google.com/store/apps/details?id=com.unitedbankofphiladelphia.mobile&hl=en_US&gl=US>

*For Business Banking*

– iPhone

<https://apps.apple.com/us/app/ubphila-business-mobile/id1631592151>

– Android phone

<https://play.google.com/store/apps/details?id=com.unitedbankofphiladelphia.biz>

If you have a question of selecting the right official apps to use on your cell phone, please contact the Bank. If possible, download the app using the link shown above. Otherwise, use a reliable app store, such as Android Apps on Google Play or Apple Apps store. Remember, always keep your mobile banking apps up-to-date.

### Don’t Save Login Information in Your Browser

Storing password is never a good idea. Although some web browsers give you the option to save your username and password within the browser — never do this for your online and mobile banking. If your phone is ever lost or stolen, this could make it easy for hackers to access your bank account.

If you’re worried about remembering your password, consider using a reputable password manager. These apps can manage usernames and passwords for multiple websites and applications, and have safety features in place to protect this information from hackers.

### Use Two-Factor Authentication

The bank uses either two-factor authentication or Token to authenticate user other than just user name and password. After user successfully log in to their mobile banking, users can also choose to use a fingerprint or face recognition to do authentication instead.

### Beware of Phishing Links

Phishing scams are one of the most common forms of cyber fraud. They work by tricking individuals into giving away private information. For example, scammers might send an email that looks like it’s from your bank or a business you’ve recently been in contact with. These emails might include a link that, once clicked upon, will install a virus on your device that can gather personal data.

Be wary of phishing scams, and never open links in email or text if you aren’t sure of their origin. Remember, you can always call the bank, if you suspect a phishing scam, and they can let you know whether or not they sent the email.

### Always Log Out

When you’re done using your mobile banking app, be sure to log out to protect your personal information, such as your email, social media, or mobile wallet, etc. If your phone were to get lost or stolen, you’d want to make it as difficult as possible to access this information.