Utilities Employees Credit Union

Mobile Banking Security Information

How UECU Protects You

UECU provides a variety of convenient tools to access your accounts, including the Mobile Banking and Home Banking versions of our *Advantages Online™* banking system. UECU maintains strict security standards to safeguard your account information, and has added to our Mobile Banking application the same security provisions that are used with our Home Banking system, including:

- A **username and password** to confirm your identity before granting account access; these are required for each Mobile Banking session.
- **Personal security questions**, which are used to authenticate your mobile device.
- A **security image** and **security phrase** pre-selected by each user to provide you verification that you are on the genuine UECU account access system.
- **Firewalls and encryption** to protect our system from intrusion or unauthorized data transmission.

Each time you sign into *Advantages Online™* Mobile Banking, your secure, encrypted banking session will begin only after you verify your identity with your username and password.

How You Can Protect Your Information and Mobile Device

Some individuals may have questions about their personal role in ensuring the security of the physical mobile phone and tablet devices they use for personal or financial activities. UECU has assembled the following tips to safeguard your mobile devices and the information you store on them.

Do:

- End each banking session by clicking on the "Sign Out" link to ensure your device is no longer displaying your account information.
- Protect all the information on your mobile device by setting a lock code or password that is required for access to the contents of your device.
- Only enter personal information on trusted websites that display a security padlock symbol and have a web address that begins with "https". This signifies a secure site that will encrypt the information you submit through your web browser.
- Download your app from Google Play or the App Store, the only two official sources for the UECU Mobile Banking app, and verify Utilities Employees Credit Union is listed as the application developer. Applications from unverified sources may contain viruses that are malicious to your device or collect personal information.
- Safeguard your mobile device with security patches, anti-virus, and anti-malware software, just as you would do for your personal computer.
- Consider installing a remote-disable application on your mobile device, which would allow you to remotely remove the personal information on your device, should it be lost or stolen. (See below for a list of these resources.)

- continued on page 2 -

Don't:

- Do not leave your phone or other mobile devices unattended.
- Do not use the *Advantages Online™* application or other mobile banking or shopping applications while your device is connected to an unsecured, public Wi-Fi network.
- Do not include your username, password, or other private credentials in an email or text message, as these could be intercepted by others.
- Do not click on a link to a login screen for Online Banking in any email that claims to be from your financial institution. Sign into your account only through your official *Advantages Online™* mobile application or through the UECU website at *www.uecu.org*.
- Do not respond with personal or account information to any emails, texts, or other messages requesting these details. Be skeptical of such requests to avoid providing information to scammers. UECU will not contact you via email or text message with any requests to provide or verify such information. Contact us directly by phone if you receive such a message.

Protection Resources for Lost or Stolen Mobile Devices

Apple Mobile Device Support

- "Find My iPhone" Application: find instructions for advance installation and details on using the application for device location and remotely wiping data at http://support.apple.com/kb/PH2696
- Lost or Stolen Apple Product Support: http://support.apple.com/kb/ht2526

Android Mobile Device Support

- "Android Device Manager" Application: find details on installing and using the application to locate your device and protect its personal data by logging into your Google account at https://www.google.com/android/devicemanager

Windows Phone Support

- Windows "MyPhone" Services: find details on mapping your phone's location and protecting its personal data at http://www.windowsphone.com/en-us/how-to/wp7/basics/find-a-lost-phone

More Resources for Protecting Yourself Online

For a list of educational resources and tips for protecting yourself online while using your computer or mobile device, visit UECU's "Protect Yourself Online" webpage at http://www.uecu.org/Information/FinancialEd.aspx?product=protectYourself