ePAPER

APCI FEDERAL CREDIT UNION

Mobile Phone Security

Protecting Your Personal and Finanical Information

Smartphones and tablets have become an essential part of everyday life, providing convenient access to banking, shopping, communicating, and other online services. However, these devices also store and provide access to sensitive information, including personal photos, emails, passwords, payment details, and financial accounts. Without proper safeguards, this information could become vulnerable to cybercriminals, identity theft, and unauthorized account access.

Fortunately, protecting your mobile device does not require advanced technical knowledge. Practicing good digital security habits, keeping your software current, and being mindful of the information you share can significantly reduce potential risks.



Understanding Common Mobile Device Security Threats

Phishing and Targeted Scams: Fraudulent emails, text messages, or social media messages may impersonate trusted organizations or individuals. These messages often encourage recipients to click on malicious links, provide confidential information, download attachments, or visit fraudulent websites.

Malicious or Untrustworthy Apps: Certain apps may contain harmful software, collect personal information without a legitimate need, or imitate legitimate services.

Outdated Software: Older operating systems, browsers, and applications may contain security weaknesses that cybercriminals can exploit to access devices or personal information.

Account Takeover: Stolen login credentials, fraudulent verification, and SIM-swapping schemes can give criminals unauthorized access to email, banking, and other sensitive accounts.

Unsafe Networks: Cybercriminals may establish fake wireless networks that resemble legitimate connections at hotels, airports, restaurants, and other public locations to deceive unsuspecting users.

Excessive App Permissions: Some applications request access to information or device features, such as contacts, photo, location, and microphones, which may not be necessary for the app to run properly.

Lost or Stolen Device: A missing smartphone or tablet can expose personal information and account access if appropriate security measures are not enabled.

Digital Tracking and Data Collection: Applications, websites, and advertising platforms may gather information about browsing habits, location, and device activity, potentially compromising personal privacy.

8 Ways to Keep Your Phone Safe

1. Keep Your Phone and Apps Updated

Software updates do more than introduce new features. They frequently include security improvements designed to address vulnerabilities and protect against emerging threats.

NCUA Federally Insured by NCUA
Equal Housing Lender

Consider the following practices:

- Enable automatic operating system updates when available.
- Regularly update applications installed on your device.
- Delete apps that you no longer use.
- Consider replacing devices that no longer receive essential security updates.

2. Secure Your Device With a Strong Screen Lock

A secure screen lock provides an important first line of defense if your phone or tablet is lost, stolen, or accessed by someone without permission.

For better protection create a strong passcode, enable fingerprint or facial recognition, configure your device to lock automatically, and avoid sharing your passcode with others.

3. Enable Multifactor Authentication

Multifactor authentication (MFA) adds an additional verification step when signing into an account. This extra layer of security can help prevent unauthorized access, even if someone obtains your password. Whenever available, enable MFA for accounts containing sensitive information.

Never approve a login notification that you did not initiate. Additionally, do not share one-time passwords, authentication codes, or verification messages with anyone who contacts you unexpectedly.

4. Create Strong and Unique Passwords

Do not reuse important passwords across multiple accounts. Use long, unique passwords. Consider using a reputable password manager. Change a password promptly if you believe it has been compromised.

5. Download Apps From Trusted Sources

Not every application available online is legitimate. Some fraudulent programs are designed to resemble familiar financial institutions, retailers, or other trusted organizations.

Only use official application marketplaces. Verify the application's developer and publisher information. Be suspicious of unexpected instructions to download an application via text, email, or phone call.

6. Review App Permissions

Applications may request access to various features and information stored on your device that are not necessary for the app to function. Granting unnecessary permissions can expose more personal information then intended. Periodically review which applications have access to your location, camera, microphone, contacts, photos, files, Bluetooth, and notifications.

7. Manage Your Location Privacy

Location sharing features can make everyday activities more convenient, from navigating unfamiliar areas to locating a misplaced device. However, allowing every application to track your whereabouts may create unnecessary privacy concerns.

Take a few moments to:

- Review which apps have permission to access your location.
- Select options such as "While Using the App" when appropriate.
- Disable location tracking for applications that do not require it.

8. Exercise Caution When Using Public Wi-Fi

Public Wi-Fi offers convenient internet access when traveling or visiting businesses. Although modern websites and applications generally use encryption to protect information transmitted online, public networks can still present security concerns.

Before connecting, consider these precautions:

- Verify the network name with the business or establishment before connecting.
- Avoid automatically connecting to unfamiliar networks.
- Check that websites use HTTPS before entering sensitive information in a browser.
- Turn off file sharing or other network sharing features when they are not needed.
- Use your cellular data if you are uncertain about the network's legitimacy.