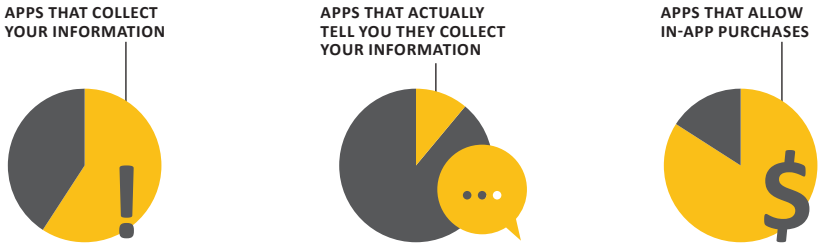
MOBILE DEVICE SAFETY

There are a number of security risks inherent in the use of smartphones and tablets, but there are some simple and common sense things you can do to protect your data and your privacy.

Be Aware: Applications Are Not Always What They Seem

The Federal Trade Commission (FTC) has found mobile application developers are not always straightforward about what their products do. According to the FTC, 59% of applications collect and share information, though only 11% tell users that; 84% of applications allow in-application purchases, opening people up to unexpected charges.



Applications that allow users to share photos that automatically "delete" themselves from recipients' devices (e.g., Snapchat) do not always work as advertised. Researchers demonstrated that Shapchat photos were not actually permanently deleted from mobile devices or Snapchat's servers.

WHAT CAN YOU DO TO PROTECT YOURSELF ON MOBILE?

Stay safe by keeping your software updated, researching the apps you use, protecting your personal information, and using secure connections...

Keep Software Updated

- Users should keep their mobile device's operating system and applications up-to-date to improve the device's ability to defend against cyber threats.

Research Apps

- Review applications' details before downloading them.
- Know what personal information applications are accessing (e.g., location, access to social networks, etc.).

Protect Personal Information

- Users should never give out personal information (e.g., full name, address, phone number, social security number, etc.) or passwords.
- Use a passcode to lock devices to avoid unwanted access.
- Users should always know where their device is to prevent theft, damage, or unauthorized access.
- Disable the geo-tagging feature to protect personal information about user location.
- For sensitive transactions (e.g., banking or shopping) look for "https://" or "shttp://" to provide secure communication via a web browser.
- Be cautious when responding to unsolicited text messages or voicemails to combat phishing.
- Encrypt sensitive data when possible.

Use Secure Connections

- Avoid using public Wi-Fi networks whenever possible.
- Turn off Wi-Fi connections when not in use.

INTERNET RESOURCES

OnGuardOnline.gov
Operated by the Federal Trade Commission (FTC), this site provides tips and technical guidance on cybersecurity issues as well as a guide for talking to children about Internet use.

StaySafeOnline.org
Offers resources on a variety of cybersecurity issues, including information on adjusting privacy settings on a number of popular platforms.