University of Kentucky
College of Agriculture, Food and Environment
Cooperative Extension Service

MONEY WISE

VALUING PEOPLE. VALUING MONEY.
MANAGING IN TOUGH TIMES INITIATIVE

Kelly May
Senior Extension Associate
(859) 562-2304
k.may@uky.edu

MAY 2019

THIS MONTH'S TOPIC:

KEEP SMARTPHONE DATA PRIVATE BY SAFELY DOWNLOADING APPS

Smartphones can make our lives easier, but they can also make our personal information more accessible in ways that we don't want.

Adware, spyware, and Trojans can infect smartphones and access your private data – which can translate into a financial problem as well as a security problem. Besides accessing your contacts and tracking your location, malware can enable someone to shop with your bank account, raise your phone bill with SMS messages, and collect passwords for all types of financial and shopping accounts you may use on your phone.

Tip 1: Use the "Official" App Store

Android may be more susceptible to malware and spyware because it is an open platform system on which many retailers can offer apps, and from many sources, not just one official store. But even if you limit yourself to only using an "official" store like the Apple Store or Google Play, it is still smart to take precautions.

Disable the installation of third-party source apps to prevent Trojans that spread through ads and other unknown sources. And know that even though the official stores have departments that work to review apps, something could still slip past.

Tip 2: Watch Out for Imposters

How do you know if an app is "safe" to download? You find out the same way you check out an investment or other financial product – you do some research.

Cooperative Extension Service
Agriculture and Natural Resources
Family and Consumer Sciences
4-H Youth Development
Community and Economic Development

LEXINGTON, KY 40546

Disabilities accommodated with prior notification.

Check out the app developer by doing a web search on what other apps they have created. Note the number of downloads and how long ago the app was published or updated. Like in phishing emails, spelling and grammar errors are a common give-away to trouble.

Read reviews, but take them with a grain of salt. If all the reviews are positive, they may be paid testimonials or posted by bots. Detailed reviews that list both good and bad features are more likely to be real user-generated feedback. While you want an app that people list positively, it's a sign that reviews are authentic if users occasionally post a negative point or question – and it's an even better sign if the developer has responded to work through the issue.

Overall, if it sounds too good to be true, it just might be.

Tip 3: Be Aware of App Permissions

What permissions does the app require to access specific functions and data? Be selective about what authority you grant – carefully review the permissions request and consider whether those permissions are really needed for that app to function.

If the app wants to access your calendar or location, it may be relaying that information to someone who wants to know where you're going – or when you're not home. If it's accessing your phone, camera or microphone, it could record at any time without your knowledge. Phone or SMS permissions also may be troublesome if criminals make calls or send messages at a charge to you. Contacts can be particularly appealing to fraudsters. Storage access can let the app read, change, or remove any files stored on the device.

If you don't want to grant the permissions, you can decline them. But if the app really needs them it may not work properly. You can change app permissions in your settings at any time. And if you suspect you've downloaded a bad app, uninstall it and see if phone performance improves.

Finally, remember that your smartphone is a computer and should be maintained by keeping system software and apps updated and by using a good antivirus and antispyware software.

Sources: Ryabova, Yaroslava. "How to avoid Android malware." Kaspersky Lab Daily Blog. Sept. 13, 2017. (Retrieved April 1, 2019) https://www.kaspersky.com/blog/android-app-security/18505/

Corrigan, Caroline. "How to check if an Android app is safe to install." AVG Signal. July 21, 2018. (Retrieved April 1, 2019) https://www.avg.com/en/signal/android-app-safety

Unuchek, Roman. "All about Android app permissions." Kaspersky Lab Daily Blog. Feb. 9, 2017. (Retrieved April 1, 2019) https://www.kaspersky.com/blog/android-permissions-guide/14014/

Empey, Charlotte. "How to tell if an Android App is safe to install." Avast Blog. Sept. 13, 2018. (Retrieved April 1, 2019) https://blog.avast.com/check-android-app-safety

Kelly May, Senior Extension Associate, Family Finance and Resource Management

Jennifer Hunter, Ph.D., Assistant Director of Family and Consumer Sciences Extension, University of Kentucky Cooperative Extension Service, (859) 257-3887; jhunter@uky.edu

Stock images: 123RF.com