Cooperative Extension Service

MONEYWI$E

VALUING PEOPLE. VALUING MONEY.

JUNE 2025

Nichole Huff, Ph.D., CFLE | Assistant Extension Professor Family Finance and Resource Management | nichole.huff@uky.edu

THIS MONTH'S TOPIC:
PROTECTING YOUR ONLINE PRIVACY

What if you used your phone at a coffee shop to check your bank account, but the Wi-Fi wasn't secure, and your bank account number and password were stolen? What if you filed your income taxes and the IRS reported they had already sent out your refund check (to someone else)? These are examples of what could happen if you don't secure your personal devices.

Digital devices provide us with information and services that make daily tasks easier. Our homes are filled with devices connected to the internet: mobile phones, tablets, computers, smartwatches, security cameras, baby monitors, thermostats, smart TVs, and smart home voice assistants. Consumers should be wary, however, as these devices have the capability to collect personal information and share it, limited only by their privacy agreements.

YOUR DATA AND HOW IT IS USED

Companies may collect data including your location, contacts, calls, messages, browsing history, fitness data, payments, and more. They might track the apps you use or the files you view or download. Some may track facial recognition or audio conversations. Some of this information might seem harmless, but other information may have personal and financial implications, such as if your bank account username and password are stolen.

PROTECTING YOURSELF

The U.S. Department of Defense has a resource for learning about threats and how to protect yourself against them. It gives tips you can use to increase your protection, including step-by-step instructions for privacy considerations on popular online services, apps, and devices.

The following are a few key dos and don'ts:

DO Be sure your home Wi-Fi is set up securely. The network name that is broadcast should not identify you or your family (for example Smith_Family_Home or 2_Dobermans). Set up strong encryption – get assistance if needed. Make sure your router's firmware is up to date.

DO Check to see if any of your usernames have been compromised. Visit https://haveibeenpwned.com/ to see if your username and password have been leaked. If so, immediately change your password for all accounts associated with it.

Cooperative Extension Service

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

MARTIN-GATTON COLLEGE OF AGRICULTURE, FOOD AND ENVIRONMENT

Lexington, KY 40506

CONTROL WHAT PERSONAL INFORMATION YOU SHARE SO YOU DON'T BECOME A VICTIM OF LOOSE ONLINE SECURITY.

DO Use a different and complex password for each of your accounts. A strong password is 10 or more characters containing a combination of upper-case letters, lower-case letters, numbers, and symbols. It is easy to use the same password over and over so you can remember it, but if it is stolen, it can expose all your accounts where you used it.

DO Enable two-factor authentication for logging in when available. This requires a third form of identification from your phone or other device. If your username and password are stolen, the thief won't be able to access your account without this other piece of information.

DON'T Don't use email or text messages to send confidential information. These services are not secure. Also, don't accept messages or open attachments from people you don't know. This is one of the preferred ways for hackers get your information.

DO Secure your social media accounts as much as they will permit.

DON'T Don't use public Wi-Fi networks, such as a restaurant, library or airport, to access anything personal or financial. If you must use them, use Virtual Private Network (VPN) software for online privacy. Some VPNs are free, and others charge a fee.

DO Secure your web browser. Review and adjust your browser's privacy settings to control what data is shared with websites and third parties. Disable features that share your location or browsing history if they are not necessary.

Control what personal information you share so you don't become a victim of loose online security. Using these recommendations to secure your phone, tablet, and computer can be the difference between minor inconvenience and a major financial setback that could take years to correct.

REFERENCES

U.S. Department of Defense (2021). The Identity Awareness, Protection, and Management (IAPM) Guide. Twelfth Edition. https://www.arcyber.army.mil/Portals/78/Documents/FactSheets/DoD-identity-protection-guide/DoD_IAPM_Guide_March_2021.pdf?ver=FDvB5WW2UB_vxPVQBJuVww%3d%3d

United States Attorney's Office, Northern District of Georgia. (2025, January 30). Protecting Yourself While Using The Internet. https://www.justice.gov/usao-ndga/protecting-yourself-while-using-internet

Contributing Author: Paul Reese, Family Financial Counseling Student, University of Kentucky
Edited by: Kelly May, Nichole Huff, and Alyssa Simms | Designed by: Kelli Thompson | Images by: Adobe Stock

Nichole Huff, Ph.D., CFLE | Assistant Extension Professor Family Finance and Resource Management | nichole.huff@uky.edu