JAN. 28

YOUR PRIVACY IN A GROWING
INTERNET OF ME

Data about you can be used in a variety of ways, sometimes in ways you wouldn't expect or even approve. That's why it's important to understand the value of your personal information and how to manage it in a safe and secure way.

DO YOUR HOMEWORK: Before purchasing any new internet-connected device, do your research. Check out user reviews on the product, look it up to see if there have been any security/privacy concerns, and understand what security features the device has, or doesn't have.

OWN YOUR ONLINE PRESENCE: The moment you turn on a new "smart" device or sign up for a new online account, configure your privacy and security settings. Most devices and accounts default to the least secure settings—so take a moment to configure those settings to your comfort level. Disable any features you don't need, such as location tracking. Make it a point to regularly check these settings to adjust them.

KEEP A CLEAN MACHINE: Keep all software on internet connected devices current to reduce risk of infection from ransomware and malware. Configure your devices to automatically update or to notify you when an update is available.

MAKE LONG, UNIQUE PASSPHRASES: Length trumps complexity. A strong passphrase is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember.

PASSPHRASES AREN'T ENOUGH: Use 2-factor authentication or multi-factor authentication (like biometrics, security keys or a unique, one-time code through an app on your mobile device) whenever offered.

LESS IS MORE: When completing a profile for an account, you don't have to fill in everything (and if you do, who is to say you have to answer honestly?). Limit what information you put online. If it isn't required, don't add it. And if a company does require information you don't feel comfortable submitting, then reconsider creating a profile with that company.

Follow the Auburn University Office of Audit, Compliance & Privacy on Twitter @AUOACP for Higher Education Compliance, Ethics & Privacy news and tips.

#PRIVACYAWARE

AUBURN UNIVERSITY IS A 2021 DATA PRIVACY DAY CHAMPION! #PRIVACYAWARE

The National Cyber Security Alliance officially leads Data Privacy Day in North America. Data Privacy Day is an international effort held annually on Jan. 28 to empower individuals and educate businesses to respect privacy, safeguard data and enable trust.

HOW TO MANAGE YOUR PRIVACY IN A GROWING INTERNET OF ME

ONLINE TRAINING: Before installing any new internet-connected device, your network installation instructions should be adhered to. But the responsibility doesn’t end there. Make sure to configure your privacy and security settings, as many devices and accounts default to the least secure settings.

ONLINE PRIVACY: The Internet has no set boundaries or a non-existent social norm. Confront your privacy and security settings. Your devices and accounts should be set up to protect your information. But, what if it isn’t? And, how do you find out? Find a trusted privacy specialist to review your online privacy settings.

STAY IN TOUCH: Keep in touch with your internet connected devices at work. You may reduce the risk of accidents and inappropriate information. Confront your devices to a systematically secure reality, as you enter them with a secure application.

CONTINUOUS MONITORING: Simply changing a password is not only enough, it’s a common practice in a password that is at least 12 characters in length. Find a trusted password manager or a password that your devices can’t remember, but you can. Find a trusted service that reports information every day. You can immediately react, but don’t have a point in your retrieval plan.

STAY SAFE ONLINE: https://staysafeonline.org/data-privacy-day

OACP Privacy Resources: http://www.auburn.edu/administration/oacp/privacyresources.php

Stay Safe Online: https://staysafeonline.org/data-privacy-day

#h i g h e r e d c o m p l i a n c e