February 2014

IN THIS ISSUE

Data Privacy Month special issue

Data privacy has been in the news lately. Cyber thieves stole credit card data and personal information of millions of Target's customers. That data included phone numbers, email and home addresses, and credit and debit card numbers, PINs and expiration dates. U.S. and British spy agencies reportedly collected users' personal data through mobile apps, including Angry Birds, Google Maps, Facebook and Twitter.

This special Data Privacy Month newsletter focuses on empowering you to protect your own privacy, take charge of your digital footprint and make privacy protection an important priority.

Why privacy matters

Should you be concerned about data privacy if you have nothing to hide? Businesses and the government can gather and analyze our personal information, and the actions we take may facilitate this. See why privacy matters when so much personal information is available online at zeroknowledgeprivacy.org/library/why-privacy-matters.

Want privacy? Don't count on it with email

Email may seem private, but it could be like a conversation in a crowded room. Texas A&M email is deemed a public record and is subject to open records requests. Although personal messages are not subject to a request even if sent via a university system, it’s best to use a private email account for personal business. Also, keep in mind most routine email are not state records subject to records retention. Delete old messages

and empty email trash regularly. *Records may not be destroyed if any litigation, claim, negotiation, audit, public information request, administrative review or other action involving the record is initiated.* Read more at u.tamu.edu/e-Discovery.

Are you a good steward of confidential information

If you have access to confidential student information, these tips help you be a good steward of the data and students' privacy:

- Use Filex to securely transfer confidential information instead of email. Its easy encryption option helps prevent inadvertent disclosures. Learn how at u.tamu.edu/howtofilex.
- Securely post grades online using eCampus (ecampus.tamu.edu). FERPA requires student grades be accessible only to individual students and other authorized personnel.
- Learn more tips at u.tamu.edu/Privacy.

Securing mobile devices against data loss

Many of us use a mobile device to read work email or access systems to conduct university business. While mobile access provides many benefits, an unsecured mobile device leaves the university - and you - open to data loss. Take steps to protect data by setting up a passcode and remote wipe. Do not store confidential information unless it is encrypted. Clear all information before donating, recycling, reselling or disposing of your mobile device. See u.tamu.edu/tUiH8dQO for more information.

Privacy on the go with VPN

Easy-to-use Virtual Private Network (VPN) protects your privacy on public Wi-Fi. VPN encrypts and secures data, shielding your online activity from hackers. For set-up instructions, go to hdc.tamu.edu/Connecting/VPN and choose your device type.

New VPN is now available for Windows RT, Chrome OS and many Android devices. The legacy VPN 3000 (vpn-master.tamu.edu) for all platforms and devices will be decommissioned during Spring Break 2014. Read more at u.tamu.edu/LlF4lkMz.

Clicked "Agree" (and didn't have a clue what you just did)

How many times have you clicked "Agree" on the terms of service to download an app or sign up for a website? Depending on the fine print, you may be giving away control over your personal information. At privacyscore.com, look up privacy risks of using many common websites. The site shows how websites stack up based on their handling and tracking of personal data.

Does everyone need to know where you are?

Location services may be convenient for finding directions, but be aware that others may be tracking your location, as well. When you use a mobile app - to play a game, update a social media profile or listen to music

– the app may be sending tracking information back to the app provider, which makes you a better target for advertisers. Your location could even be used for criminal purposes, such as theft or stalking. Use caution when apps ask for location information. Check privacy settings on your mobile devices and online accounts. These links can help you fine tune privacy settings on mobile devices. Note: some privacy settings may affect services of "free" apps that rely on ad revenue.

- Apple: howto.cnet.com/8301-11310_39-57613288-285/four-ios-7-privacy-tips
- Android: www.mobilesecurity.com/articles/552-how-to-manage-privacy-settings-in-android

---

If you have questions regarding privacy issues at Texas A&M University, please contact Jeff McCabe at the Office of the Chief Information Security Officer.

The PossibilITies newsletter is delivering more news and useful tips that help put technology to work for you. If you have questions about an IT service, contact Help Desk Central at 979.845.8300 or helpdesk@tamu.edu.

Tell us what you think about this newsletter by emailing tamu-it-coms@tamu.edu.