5 Tips for Keeping Your Data Safe

Information Security Office
January 2019

Do your New Year’s resolutions include being more secure in the IT sense?

They should ? hackers and scammers specifically target the UA community.

Data Privacy Day [1] is this coming Monday, making now a great time to implement these tips from the UA Information Security Office [2] into your daily life.

1. **Be wary of emails.** Scammers are getting more clever and more targeted with their phishing. Recent phishing emails [3] sent to campus include a sophisticated academic fellowship invitation and an email from "President Robbins" with a gift card offer. The Information Security Office's phishing alerts [4] keep you up to date with recent campus scam attempts.

2. **Be wary of phone calls.** Scammers also use emotional manipulation to get money and/or information from you over the phone. It’s good to keep in mind that the IRS will never call you about an important notice; such notices are sent to mailing address. Likewise, Microsoft will not call you about an issue with your system. If someone unknown calls you at work, remember not to divulge any internal, confidential or regulated data [5].

3. **Use updated anti-virus/anti-malware software.** Your information technology staff should have Sophos Central [6] installed on your work machine. Make sure you use security software at home as well. Most internet service providers provide this service to their customers. If you don’t have a service, Sophos Home [6] is a free option. Smartphones and tablets [7] need anti-virus and anti-malware software, too, as they are small computers that we carry with us everywhere.

4. **Keep software up to date.** Those notices you get to update your system and your software are about more than new features. Software companies also patch bugs and security holes with every release. The longer you go without updating, the longer your machine is vulnerable to getting hacked.

5. **Lock your device screens.** You should always keep an eye on your laptop or phone. But if it does get stolen, the thief won’t get your personal information if you’ve locked your screen with a passcode, thumbprint, or other lock. It’s also a good idea to lock your work computer screen or log off if you’re going to be away from your desk for a while.

Here are a couple of additional tips for a security step you’re already taking. UA systems are now protected by two-factor authentication for all logins ? NetID+ [8]. Here’s how to make the process as easy as possible:

- **Fewer steps.** Are you seeing the NetID+ screen more often than you should? When you see the screen asking you to choose your authentication option, click the box that says "Remember this device for 30 days" before selecting an option. Note: You need to do this for each browser you use.
• **Faster logins.** Install the Duo app on your smartphone and/or tablet. Or buy a Yubikey hardware token. These options take a little more work to set up, but then logins are as easy as one click of a button. The [24/7 IT Support Center](https://it.arizona.edu/get-support) or your IT staff will be happy to help you with setup.

Visit [security.arizona.edu](https://security.arizona.edu) for more information and tips. If you have questions or need help with NetID+, antivirus, or other UA services, contact the 24/7 IT Support Center at 520-626-8324 or open a chat at [support.arizona.edu](https://support.arizona.edu).

**Source URL:** https://uaatwork.arizona.edu/lqp/5-tips-keeping-your-data-safe

**Links**
[1] [https://staysafeonline.org/data-privacy-day/](https://staysafeonline.org/data-privacy-day/)
[2] [https://security.arizona.edu/](https://security.arizona.edu/
[3] [https://uaatwork.arizona.edu/uanounce/increased-email-phishing-activity-reported](https://uaatwork.arizona.edu/uanounce/increased-email-phishing-activity-reported)
[4] [https://security.arizona.edu/phishing_alerts](https://security.arizona.edu/phishing_alerts)
[5] [https://security.arizona.edu/content/data-classification-and-handling-standard](https://security.arizona.edu/content/data-classification-and-handling-standard)
[6] [https://softwarelicense.arizona.edu/sophos-central](https://softwarelicense.arizona.edu/sophos-central)
[7] [https://mashable.com/roundup/best-antivirus-for-android/#R0wEMmPR.OqZ](https://mashable.com/roundup/best-antivirus-for-android/#R0wEMmPR.OqZ)
[8] [https://netid-plus.arizona.edu/](https://netid-plus.arizona.edu/)
[9] [https://it.arizona.edu/get-support](https://it.arizona.edu/get-support)
[10] [https://support.arizona.edu/](https://support.arizona.edu/)