Stay Safe From Hackers in 2018 With These 10 Tips

University Information Security Office
January 2018

Yahoo!, Uber, Equifax. Some huge data breaches hit the news in 2017. The details varied but the consequence was the same: personal information was compromised.

This year, resolve to protect yourself. To help you keep your resolution, the University Information Security office suggests following these 10 tips to protect your Social Security number, bank account and credit cards, as well as sensitive University information.

1. **Think before you click.** Phishing email [1] is the No. 1 way that information gets compromised. Never respond to an email that asks for your password or other personal information. Be wary of links and attachments in email.

2. **Back up your data.** Whether it's ransomware, a virus or just a worn-out hard drive, you don't want to lose access to your information. Use Box@UA [2] or Office 365 [3] for cloud storage. Invest in an external hard drive, and back up your data to ensure that it is there when you need it.

3. **Create strong passwords.** Gone are the days when it was necessary to create passwords that are hard to remember (such as Qx39#!vk). Switch to using pass phrases [4] wherever possible. They are easier to remember and much harder to guess.

4. **Don't use the same password everywhere.** If a data breach reveals your password, scammers will try it on other services. Get a password manager like LastPass, Dashlane, 1Pass or KeePass that will remember all those different passwords for you.

5. **Use two-step verification wherever it is available.** While passwords are an important line of defense for your sensitive information, they are no longer enough. Use two-step verification (such as a text message code confirmation) if it is available, especially on banking and credit card accounts, social media and email.

6. **Sign up for Global NetID+.** The University's two-step login protection is in front of Office 365 email and will be added to more services this year. Enable Global NetID+ now for full protection in front of all services, in case your NetID password is compromised.

7. **Update your system and software.** Hackers eventually find holes in any system, browser or software, which is part of the reason companies send out upgrades and patches. Stay current to protect yourself from hackers testing for old vulnerabilities.

8. **Use secure wireless connections.** When you are on campus, use UAWiFi [5], the University's fast, secure wireless network. When off campus and using public WiFi, use the UA's VPN [7] (virtual private network).

9. **Use antivirus tools.** Keep a current subscription to protect you as new threats show up. The University provides Sophos [8], which you can use on your home Windows and Mac computers (yes, Macs need antivirus, too).

10. **Lock down your devices.** Don't leave your laptop or device somewhere "just for a minute." That's all the time it takes for it to disappear. Just in case, add a lock: a password for your computer screen, a passcode or a thumbprint or facial recognition for
your phone or tablet. Encrypt your devices if possible, so that your data will be secure even if your machine "walks off."

Find more tips and information at [security.arizona.edu](https://security.arizona.edu) [9]. 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) [10].

**Source URL:** [https://uaatwork.arizona.edu/lqp/stay-safe-hackers-2018-these-10-tips](https://uaatwork.arizona.edu/lqp/stay-safe-hackers-2018-these-10-tips)

**Links:**
[1] [https://security.arizona.edu/phishing](https://security.arizona.edu/phishing)
[2] [https://it.arizona.edu/service/boxua](https://it.arizona.edu/service/boxua)
[3] [https://it.arizona.edu/service/microsoft-office-365](https://it.arizona.edu/service/microsoft-office-365)
[4] [http://security.arizona.edu/password-security#use](http://security.arizona.edu/password-security#use)
[5] [https://netid-plus.arizona.edu/](https://netid-plus.arizona.edu/)
[6] [https://it.arizona.edu/service/uawifi](https://it.arizona.edu/service/uawifi)
[7] [https://it.arizona.edu/service/ua-virtual-private-network-vpn](https://it.arizona.edu/service/ua-virtual-private-network-vpn)
[8] [https://softwarelicense.arizona.edu/sophos-endpoint-security-and-control](https://softwarelicense.arizona.edu/sophos-endpoint-security-and-control)
[9] [https://security.arizona.edu/security-faculty-and-staff](https://security.arizona.edu/security-faculty-and-staff)
[10] [https://support.arizona.edu/](https://support.arizona.edu/)