Taking a summer vacation is a great time to relax and decompress from the previous school year. But in 2017, many of us stay connected while “getting away from it all.”

This month’s newsletter highlights things to be aware of as you enter unfamiliar network waters, including many tips for your identity and information safety. We also introduce you to Office 365, and provide tips on keeping data secure during the migration!
COMMON THREATS WHILE TRAVELING

Pickpocketing is no longer the largest concern when traveling to tourist locations. Keep both physical and cybersecurity in mind when traveling to ensure that you and your data remain secured. Below are a few of the most common threats while traveling with wireless devices.

- **Unsecured wireless networks** – Connecting to public wireless networks can make mobile devices unsecure and allow cyber criminals access to any internet-enabled device.
- **Publicly accessible computers** – Public computers available in libraries, hotel business centers, or cafes cannot be trusted as secure computers. Such machines are easily infected with malicious software such as keyloggers that can steal personal information.
- **Physical theft of devices** – Thieves target travelers and often check hotel rooms during meal times for unattended laptops. Those attending conferences should be especially wary.

Before You Go:

- **Update your mobile software** - Keep devices up-to-date to improve the device’s ability to defend against malware.
- **Keep it locked** - Lock your device when you are not using it with strong PINs and passwords when not in use.

While You Are There:

- **Stop auto connecting** - Disable remote connectivity and Bluetooth to prevent automatically connecting to unsecure networks or other devices.
- **Think before you connect** - If you MUST connect to public wireless (e.g., airport/plane, hotel, cybercafé), avoid performing any tasks that touch sensitive information, such as online banking or shopping. Use the UA VPN whenever possible to create a secure channel around your data.
- **Guard your mobile devices** - Never leave your device(s) unattended in public places.
- **Actively manage location services** - Location tools are useful when navigating a new city, but disable them when not in use.

How to Make Your Life Easier with NetID+

**What is NetID+?**

NetID+ adds a second layer of security – a code sent by text, phone, app, or device that authenticates a login beyond the password, protecting accounts in the event of password compromise.
Make NetID+ Work for You
Securing your personal information with NetID+ can be easy. To make NetID+ work for you, add multiple devices to your NetID+ account. Consider doing at least two of the following so that you are always prepared:
1. Download Duo Mobile on your smart phone or tablet for “push” notifications.
2. Add another cell phone (if you have one available) that accepts SMS (text message) passcodes.
3. Add landlines, such as your work and home phone, so that you can easily authenticate by answering the phone and pressing “1”.
4. Use a Yubikey hardware token to generate passcodes.
5. Print out passcodes, just in case.
6. Enable Global NetID+ to ensure that your information is secured everywhere that WebAuth logins are used. *NOTE: If you do not enable Global NetID+, your data is not secured on systems that do not require NetID+.*

What is a Yubikey, and Where Can I Get One?
A Yubikey is a hardware authentication device that can serve as your second method of authentication. These handy devices plug into your computer via a USB port. These can also be used with smartphones and tablets if you have a USB adaptor to plug into your device. Yubikeys can make NetID+ much easier to use when traveling, especially if you are traveling internationally.
- Yubikey 4, Yubikey 4 Nano and Yubikey Neo will all work with NetID+.
- Your YubiKey will need to be configured to use with your NetID+ account. Once this is complete, you can use it every time you log in to WebAuth or the UA VPN.

Visit the [NetID+ support and how-to page](#) for full documentation on making two-factor authentication easy.

---

**Helpful Facts and Safety Tips for the Migration to Office 365**
- Student workers will still keep their CatWorks accounts, and will use UAConnect365 the same way faculty and staff do.
- UA Office 365 accounts are free for students as long as they are actively enrolled in the University.
- Users are offered 1TB OneDrive storage that is in addition to the Box@UA storage that students and staff are already offered.
- Downloading Outlook 2016 will provide you with the best performance in this transition.
- You will need to change your NetID+ password if you haven’t changed your password since March 6, 2017.
- You will also need to sign up for NetID+ for this transition, and we highly recommend signing up for Global NetID+ for an extra layer of protection.
- Be sure to have a new password and sign up for NetID+ before you leave for the summer to avoid any access problems while you are away.

Find more information on migrating to Office 365 on the [UA IT website](#).