Last month’s newsletter focused on securing your mobile devices.

This month, we delve a little deeper, including covering security tips to follow when traveling, especially internationally.

We will also cover ransomware: what it is, and how to protect yourself and your data against it.

Finally, we will tell you about UAGuest, the new guest wireless service available to campus.

MOBILE DEVICE SECURITY, PART 2

Last month, we introduced our first 5 tips for securing your mobile devices. They are:

1. Lock it
2. Install security software
3. Manage applications
4. Use a “Find Your Phone” tool
5. Backup – and then backup again
Following are the remaining tips.

6. **Don’t Automatically Connect**
   - Automatic connections to WiFi, Bluetooth, and NFC (Apple Pay, Android Pay, etc) items can be used to access your data without your permission. It isn’t worth the risk – disable these when not in use.

7. **Keep It Behind Bars – No Jailbreaking!**
   - Jailbreaking is the process of removing software restrictions by the device manufacturer. While this may increase some functionality, it makes it harder to install necessary updates. When these updates go uninstalled, hackers have a known way to enter your device.

8. **Beware of Email, Voice, and Texting Scams (AKA Phishing, Vishing, and Smishing)**
   - Social engineering is taken to a whole new level with mobile devices, especially smartphones. Hackers can try to trick you via email, voice, or text message. Do the following, regardless of how you are receiving communications:
     - Always check credentials of anyone contacting you, regardless of the method of communication.
     - Look for spelling and grammatical errors.
     - NEVER provide personal information via email or text. Only give information over the phone if you initiated the call to a verified legitimate source.

9. **Privacy Everywhere**
   - Check your privacy settings.
   - If an app uses your location and you don’t think it needs to, ensure that you turn that setting off.
   - Occasionally go through your previous WiFi networks and remove ones that you no longer connect to in order to make your physical location harder to pinpoint.

10. **Use Secure WiFi**
    - Only use secure WiFi, such as UAWiFi, VPN, or your secure, password-protected WiFi at home.
    - Protect yourself by not connecting to public WiFi networks or using a VPN when connecting.

For more information, visit our [Mobile Device webpage](https://example.com/mobiledevice).

---

**SECURE TRAVEL WITH MOBILE DEVICES**

Approach securing your devices and data when traveling as you would a painting a house. Invest time up front (e.g., put down drop cloths, tape around windows and edging) and the job will go much smoother and most likely without incident.

Along with our Top Ten Mobile Device Security Tips, use the following checklist to help make your trip more enjoyable, ESPECIALLY if you are traveling internationally.

**BEFORE YOUR TRIP**

- **Travel light:** If you don’t absolutely need a device, leave it at home.
- **Go disposable:** Consider purchasing a “burner” or disposable phone in your destination country.
- **Travel with “clean” devices:** If you must take your own device, remove all regulated and confidential data.

**NOTE: DO NOT BRING REGULATED UNIVERSITY DATA OUT OF THE COUNTRY UNLESS YOU HAVE RECEIVED APPROVAL FROM APPROPRIATE COMPLIANCE OFFICERS.**

- **Use strong passwords and device timeouts** for all accounts and devices that you will use overseas.
- **Sign up for Global NetID+ Two-Factor Authentication:** Doing so decreases the risk that your sensitive personal information will be accessed, should your UA NetID become compromised while traveling.

**Use the UA Virtual Private Network (VPN):** UA’s VPN provides a secure connection from your computer to the Internet, and can be used on multiple platforms and devices.
During Your Trip
- Keep track of what credentials you use while traveling.
- Keep your technology with you or securely hidden and locked.

After Your Trip
- Change passwords for all services you accessed while away.
- Scan your devices for malware.

For more tips on travel security, visit our Travel Security webpage.

The Rise of Ransomware
Hackers and scammers increasingly select ransomware as their weapon of choice. You have probably heard the term. But what is it, and what can be done to mitigate the risk and pain that come along with this nasty form of malware?

What is Ransomware?
One of the best definitions we have seen for ransomware comes from techtarget.com: “malware for data kidnapping, an exploit in which the attacker encrypts the victim’s data and demands payment for the decryption key.” Malware infects the computer in a variety of ways, such as infected websites or phishing emails.

What Can Be Done?
Ransomware attacks are on the rise, and are predicted to be one of the biggest threats in 2016. Be sure to put security layers between your data and the bad guys to protect yourself from this pernicious beast.

1. **Install security software on all your devices.** Sophos Endpoint Security and Control is available to all faculty and staff, and can be downloaded on the University’s software license website.
2. **Backup your data.** Backing up your data to an external hard drive and/or cloud service provides you with some peace of mind, should your device become compromised, stolen or lost.
3. **Don’t fall for a phish.** Phishing is ubiquitous for one reason: it’s effective. Learn how to spot a phish by visiting our phishing tips webpage, and report phishing emails to UA Information Security.

Learn how to protect yourself from ransomware.

Visit our website for security tips and awareness information.

- Security Building Blocks
- Phishing
**UAGUEST IS HERE!**

On April 22, University Information Technology Services launched UAGuest, a new wireless network for visitors, to significantly improve the university’s wireless network security and mitigate unauthorized access to campus resources.

Unlike the old UAPublic guest wireless network, UAGuest requires authentication with a user name and password.

Campus visitors can select UAGuest from the wireless options on their device, and establish an account valid for five days by entering a username and cell phone number. After five days, guests will need to establish a new account.

UAGuest and UAPublic wireless networks will remain available in parallel until **May 22**, at which time UAGuest will replace UAPublic.

**NOTE:** UAGuest is an unsecured network; do not send private information, such as credit card numbers, when logging on to this network. Faculty, staff and students should continue to use UAWiFi for fast, secure wireless access on campus.

For more information and instructions on UAGuest, visit UITS’ [Campus Visitors webpage](#).

---

**Would you like to promote security awareness in your department?** Download our **custom screensavers!**

---

**STAY INFORMED ON**

**INFORMATION SECURITY**

**ISSUES**

**TRENDS**

**ALERTS**

Sign up for [UA Information Security’s listserv](#). Open to all faculty and staff.