UNIVERSITY OF DELAWARE | Research Office

Charles G. Riordan, Ph.D.
Deputy Provost for Research and Scholarship
Professor, Chemistry and Biochemistry

124 Hullihen Hall
Newark, DE 19716
Phone: 302-831-4007
Email: riordan@udel.edu

TO: University Faculty and Staff

FROM: Dr. Charles Riordan, Deputy Provost for Research & Scholarship

DATE: December 14, 2015

SUBJECT: University Procedure for International Travel with Electronic Devices

The purpose of this memorandum is to remind and inform University of Delaware (UD) employees of the states-of-nature and UD expectations that exist when traveling internationally with mobile devices, laptop computers, personal-digital assistants (PDAs) and other electronic devices.

Consistent with the guidelines offered by the Office of the Director of National Intelligence, U.S. National Counterintelligence & Security Center (NC&SC) (www.ncsc.gov/industry/travel/index.html), University personnel who are traveling internationally should be aware that:

1) In most countries, travelers should have no expectation of privacy in internet cafes, hotels, offices or public places. Hotel business centers and telephone networks are regularly monitored in many countries. In some countries, hotel rooms are often searched.
2) All information that you send electronically by FAX machine, PDA, computer or telephone can be intercepted. Wireless devices are especially vulnerable.
3) Your movements can be tracked using your mobile telephone or PDA, and the microphone in your device can be turned on even when you think that it is turned off. To prevent this, remove the battery.
4) Malicious software can be inserted into your electronic device through connections you use. This can also be done if your device is enabled for wireless. When you connect to your home server, the malware can migrate to your home system and/or the University, can inventory your system, and can send information back to the individuals who inserted the software.
5) Malware can be transferred to your device through thumb drives (Universal-Serial Bus (USB) sticks), computer disks … some of which you may have been given as “gifts”.
6) Transmitting sensitive information from abroad is risky.
7) While corporate or government officials may be most at risk, it incorrect to assume that you will not be targeted.

8) Intruders are skilled at posing as someone you trust in order to obtain personal or sensitive information (i.e., phishing).
9) If customs officials demand to examine your device, or if your hotel room is searched while your device is unattended in the room, you should assume your device has been compromised.

To mitigate these threats, again consistent with NC&SC guidelines, when traveling internationally, University personnel should:

1) Take only necessary devices.
2) Take only needed information, including sensitive contact information. Consider the consequences if your information were stolen or otherwise compromised.
3) Back up all information you take, and leave the backed-up information at home.
4) If feasible, use a different mobile telephone or PDA from your usual one, and remove the battery when not in use. Have your device examined by your UD information technology (IT) support-personnel when you return.
5) Monitor official cyber security alerts from www.onguardonline.gov and www.us-cert.gov/cas/tips.
6) Prepare your device for international travel (prior to departure) by:
    a) Creating a strong password (numbers, upper and lower case letters, special characters – at least eight characters long). Never storing passwords, telephone numbers, or sign-on sequences on any device or in its case.
    b) Changing passwords at regular intervals, and as soon as you return.
    c) Downloading current, up-to-date antivirus protection, spyware protection, operating system security patches, and a personal firewall.
    d) Encrypting all sensitive information on a device. (Note that in some countries, customs officials may not permit you to enter with encrypted information.)
    e) Updating your web browser with strict security settings.
    f) Disabling infrared ports and features you don't need.

While travelling internationally, you should:

1) Avoid transporting devices in checked baggage.
2) Use a digital signature and encryption when possible.
3) Don't leave your electronic devices unattended. If you stow a device, remove the battery and subscriber-identity module (SIM) card, and keep them with you.
4) Don't use thumb drives given to you – they may be compromised. Similarly, don't use your own thumb drive in a foreign computer. If you must do either, assume your device has been compromised, and have it cleaned as soon as possible.
5) Shield passwords from view. Don't use the "remember me" feature that is found on many websites … retype the password every time.
6) Be aware of who is looking at your screen, especially in public places.
7) Terminate connections when you are not using them.

8) Clear your browser after each use, delete history files, caches, cookies, URL and temporary internet file.
9) Do not open emails or attachments from unknown sources. Don't click on links in emails. Empty your "trash" and "recent" folders after every use.
10) Avoid Wi-Fi networks. They are insecure, and maybe controlled.
11) If your device or information is stolen, report it immediately to UD and the local US embassy or consulate.

Upon your return from international travel, you should:

1) Change your password.
2) Have your UD IT support-personnel examine your device for the presence of malicious software, if you suspect that it may have been compromised.

If you have questions, contact the Research Office at UDResearch@udel.edu or (302) 831-2383. Additional information regarding "Travel Best Practices for Both Domestic & Abroad" is provided by UD Information Technologies at https://www.udel.edu/it/security/bestpractices/travel.html.