HARVARD
Information Security

Advisory for Travelers
Updated February 6, 2014

This advisory is intended to assist members of the Harvard community who are going to be traveling with portable computing devices including laptop computers, PDAs, tablets and smart phones.

General Recommendations

You should assume that your computing device will be lost or stolen. A 2008 study reported that 12,000 laptop computers go missing or are stolen each week at United States airports, 40% of them at security checkpoints. This means that you need to protect any confidential information that might be on the device.

The probability that your portable device will be lost also means that you should ensure that you do not have the only copy of important information on the portable device. Any information generated or collected during your trip should be regularly copied back to a secure location at Harvard or elsewhere. The transfer should be encrypted if the information is confidential. A simple way to do this is to encrypt the information and email the encrypted file to a University email account.

Should your device be lost or stolen, it is good practice to minimize the amount of information that can potentially be disclosed or that needs to be reported. Before you travel, determine if you can reduce the information contained on the devices you will bring. Perhaps you can move anything not associated with this trip to a secure archive in your office.

In general, always maintain the most recent version of all operating system and application patches on your devices. Keep your endpoint security tools such as antivirus and firewalls enabled and up to date.

If your device is lost or stolen, please report the issue using the Report Issues or Incidents link.

Harvard Security Policies

1. Harvard policy requires that all University-owned laptops be password protected and encrypted.

   See http://security.harvard.edu/book/28-confidential-information-harvard-computing-devices

2. Harvard policy also requires that no high risk confidential information (HRCI) be stored on a user computer, including portable devices such as laptops, even if the device is encrypted.

   See http://security.harvard.edu/book/11-storing-high-risk-confidential-information

Harvard Research Data Security Policies

In addition to the requirement for University-owned laptops and personal devices to be encrypted, Harvard has specific data gathering policies intended to protect the confidentiality of research subjects. Under no circumstances can high risk confidential information about people, such as SSNs,

be stored on a laptop. See the Harvard Research Data Security Policy and other Research policies at http://www.security.harvard.edu/focus-research for specific advice for researchers gathering confidential data in the field.

Security Considerations for International Travelers

There are some additional factors to consider if you are traveling internationally. We highly encourage you to read the following especially if you are travelling to a location known to have an active cyber-criminal community or where you would be subject to surveillance.

Encryption

The US government export regulations includes an exemption for the personal use of encryption technology on portable devices except if the travel is to one of the countries that the US has designated as supporting terrorism (as of July 30, 2010 this included Cuba, Iran, North Korea, Sudan, and Syria). You must remove any encryption technology if you will be traveling to these countries. (See www.gpo.gov/bis/ear/pdf/740.pdf for more details.)

Some countries have their own regulations restricting the use of encryption. The most prominent are France, South Africa, China and Russia. See http://www.cryptolaw.org for an unofficial list of national encryption related laws.

Passwords

A number of countries have laws that require you to produce a password if requested by law enforcement officials. In some of these countries, refusal to provide the password can result in arrest and time in jail. US Customs occasionally searches laptops when a traveler returns to the country. They have been known to retain laptops for further analysis if a traveler refuses to unlock the system.

If at any point on your trip, you are prompted to surrender your password or device to a law enforcement official, please do so. Harvard's criteria for protecting and securing information on devices should never put your own health and safety at risk.

If you need to remotely-access Harvard resources (such as University email) when travelling, change your password prior to the trip and change it again on your return. If your password is compromised, changing it proactively can potentially reduce the window of opportunity of the attacker to exploit the information accessible using your password.

For additional security when you travel, you may want to consider using a temporary mail account on a public mail server such as Gmail or Hotmail. If the mail service allows for multi-factor-authentication, please choose to use the additional authentication criteria.

HARVARD
Information Security

Temporary devices

Consider if you can use a temporary device for the duration of the trip. Minimize the information contained on the device. On your return, print any files changed or created on the trip and wipe the device completely or restore it to the factory default.

Kiosks and Public Wi-Fi

Never trust public wi-fi, please use the Virtual Private Network (VPN) client on your device if it is available. A VPN connection will encrypt your transmission and ensure it remains confidential when traversing the public network. If your device is a smartphone or tablet that automatically checks your email, consider disabling that feature for the duration of your trip.

If you need to use a public or shared resource such as wi-fi or a kiosk, we encourage you to refrain from accessing a University resource or e-Commerce site. If you use your username and password on an untrusted workstation or network, they may be intercepted or stolen and the confidentiality and security of any information you access may be exposed.

International Travelers: Register Your Itinerary

Harvard students, faculty, and staff who are traveling abroad are strongly encouraged to register their travel itineraries in the Harvard Travel Registry, so that Harvard may contact travelers quickly in an emergency. To register, visit www.traveltools.harvard.edu.