Glossary

Anti-virus – program that looks for and tries to stop known malware.

Firewall – program that prevents unsolicited connections to your PC.

Malware – any evil software designed to take over your computer.

Virus – malware designed to spread without user action.

Trojan – malware that hides itself inside another program.

Bot – malware providing interactive control of your PC to criminals.

Crypto locker – extortion malware that encrypts your files until paid.

Phishing – email to fool you into giving away money or passwords.

RESTRICTED Info – Information that can cause financial loss like: Social Security Number, Credit Card Number, Bank Account & PIN…

SPAM – unsolicited email offers to sell you goods or services.

Updates – software patches to close security holes and fix bugs.

Resources

Computer Help	+1 310 506 **4357** (**HELP**)
Information Breach	+1 310 506 4040
Lost/Stolen Computer	+1 310 506 4442
Grad Campus Support	bit.ly/peppgradtech
Seaver Faculty Support	community.pepperdine.edu/it/helpdesk/techliaisons.htm
Tech Central Support	community.pepperdine.edu/it/students/
	+1 310 506 4811
Good password?	mypassword.pepperdine.edu
Anti-phishing tips?	phishing.pepperdine.edu
Copyrighted files?	filesharing.pepperdine.edu
Large/Secure file xfer	attachments.pepperdine.edu (up to 20Gb)
Pepperdine IT info	community.pepperdine.edu/it/az

ISO Quick Reference Guide 7

The international experience is one of the most memorable times in your Pepperdine University career. Protect your account, data, computer or device from being compromised.

INTERNATIONAL

Secure Computing

Secure computing overseas:

1. Don't input your ID + Password on a public computer.
2. Keep your devices up-to-date with security patches.
3. Exchange files using the network rather than USB drives.
4. Use secure network connections like https. Don't accept 'proceed anyways' prompts on secure connections.
5. Use anti-virus on your computer.

Filesharing

Don't share or download copyrighted media without authorization. Penalties are different (and often not as lenient) overseas.

Support

International Programs Students, consult with your program staff on IT issues before contacting the Malibu campus

REPORT LOST or STOLEN COMPUTER or DEVICE TO:
Department of Public Safety
310 506 4442

REPORT SUSPECTED LOSS OF Social Security, Credit Card or Health Care records to
Information Security Office (ISO)
310 506 4040 or 310 506 4357

I love travel, but I'm aware that there are more threats to security and greater risk if something goes wrong while overseas. Just like a good itinerary, a few preparations make for peace of mind.

-- Kim Cary, Chief Information Security Officer and traveller

Before you go:

1 - Prepare to control your ID, password and computer

All Pepperdine University services including Google Apps use secure ID/password entry, so you're safe even on international WiFi. However, a computer you use at a friend's home or public café may be compromised. Restrict your use of borrowed/public devices to information searches and don't use them to log in. Also,

1. Keep an eye on your devices; sounds like common sense, but especially needed abroad.
2. Set a good password on your computer and your mobiles.
3. Configure any 'find my device' services before you go abroad; they not only help you find a lost computer or device, but can also erase them if stolen.

2 - Perform any security updates

Students. Read browsercheck.pepperdine.edu and click the 'Check Your Browser Now' button.

Faculty & Staff. Take your University computer to tech support and have them make sure Device Management is configured. Browsercheck is good for you, too!

3 - Set a password and locking screensaver

Make sure you have set up a good passphrase (not just a PIN) on all your computers and mobiles. Set a timeout to a locking screen saver. Apple's TouchID™ is good protection, if you have a passphrase behind it. The security office recommends setting auto-wipe for 10 consecutive bad mobile passwords.

4 - Do a backup

If your device is stolen or your hard drive crashes, will you lose years of work, pictures and email?

Activate the over-the-air backup service for your mobile device so you don't lose vital data if you lose the phone or tablet. Know the limitations of such a service and follow the manufacturers recommendations for backups and syncing.

Computer backup strategies:

- Copy academic & personal files to Pepperdine Google Drive – UNLIMITED storage
- Consider purchasing a $50-100 USB hard drive to use with Mac Time Machine or Windows Backup – if you can, leave a copy of that backup here in the U.S., while using cloud backup like Pepperdine Google Drive to backup files you create overseas.

5 - Activate Anti-virus

It isn't invincible, but anti-virus can help against well-known malware. Sophos and Avast offer free anti-virus for Mac. AVG & Microsoft offer free AV for Windows. Install it and make sure it's updating.

6 - Set up the guest account for loaning to friends

If someone needs to borrow your computer for a short time, don't give him or her full access to your files, email, saved website passwords, etc. Log out and let them log in with the guest account – they will be prevented from accessing your documents. For both Mac and Windows the guest account must be turned on to be used. Info at: http://bit.ly/peppcompguest

7 - Check in with your tech support before going abroad

Students. You really do NOT want to have issues with illegal file sharing overseas. Sure, at Pepperdine we want you to do the right thing, but there are other things to consider. Not only could swamping your house's network connection with illegal downloads make you seem selfish, but getting the house director a fine for uploading copyrighted files (true story) could get you sent home. Check in with Tech Central and let them help make sure you don't have any illegal filesharing software on your machine. They can also help make sure you are set up with all the preparation steps in this pamphlet and answer your questions.

Faculty & Staff. Make an appointment with your tech support a couple weeks before going abroad. He or she will likely have specific recommendations and checks they want to do for you before you go overseas. Also, they will be able to answer your tech questions about overseas, maybe even some you didn't think to ask!

Stateside again. Often the tech support abroad configures your device in a way that it can't get on the network when you're returned from abroad. Plan to leave a little time before the term on your return to test your connection and if it isn't working check in with tech support.

While abroad:

- Keep an eye on your devices; theft is a problem abroad, more than on campus.
- Do NOT work with RESTRICTED information on your computer while abroad.
- Use network transfers like attachments.pepperdine.edu or Pepperdine Google Drive to collaborate, rather than USB sticks, which can carry malware from computer to computer.
- Software that allows you to circumvent country controls on social media, etc. often contains malware – be wary of using this software.
- Faculty & Staff can use the VPN to access Pepperdine LAN resources while abroad. It does NOT protect or encrypt your general Internet traffic, just to/from the Pepperdine nets.
- All Pepperdine services, like Wavenet, Google Apps, Courses, email.pepperdine.edu are available from all International Programs campuses.