MESSAGE FORM

(INSTRUCTION: FILL-UP BOXES INSIDE DOUBLE LINES ONLY)

FOR COMCEN/SIG USE

PRECEDENCE ACTION/PRECEDENCE INFO
"PRIORITY"

FM: CG, PA

TO: All Unit Commanders
Attn: G6/Signal Officer/IS Officer

INTERNAL: All G-Staff, Personal, Special & Tech Staff, C, AOC/SAGS/XA

INFO: CSAFP
Attn: J6

GROUP:
15 October 2015

SECURITY CLASSIFICATION:
CONFIDENTIAL

ORIGINATOR:
6/CMB 1510-20-2015

1. References:

   a. Command Guidance
   b. Cybersecurity Awareness
   c. VAPT and PANET Monitoring Result

2. As per above references, forwarded is the Cyber Security Bulletin number 029 with topic regarding **How Can I Make Sure My Laptop Is Secure When I Travel With It?**

3. ITR, all concemed G6/Signal Officers/Information System Officer/NCOs are reminded to include this information as part of TI & E on all of its subordinate units as part of enhancing the Cyber Security Awareness of the Philippine Army.

4. For information and widest dissemination.

DRAFTER'S NAME AND TITLE	**PHONE NR:**
MAJ JOEY T FONTIVEROS (INF) PA Chief, CMB, OG6, PA	6630
RELEASER'S NAME AND TITLE	
COL VENER ODILON D MARIANO GSC (SC)PA AC OF S FOR CEIS, G6, PA	

HEADQUARTERS
PHILIPPINE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEMS, G6
Fort Andres Bonifacio, Metro Manila

6/CMB

15 October 2015

CYBER SECURITY BULLETIN

Cyber Security Bulletin: #029

How Can I Make Sure My Laptop Is Secure When I Travel With It?

Hitting the road with your computer opens the doors to a whole world of potential security problems, both physical and software-based, but don't worry, they're all manageable. Remember, the weakest link in your security will usually be you — as long as you don't put yourself, your computer, or its data at undue risk, you should be just fine even if you have to work from a library or a cafe, or connect to whatever Wi-Fi you find to get some work done. Here's what you can do to protect yourself.

Keeping your gear safe starts with protecting it physically. Of course, if someone is really gunning for your laptop, they'll probably find a way to get their hands on it, but that doesn't mean you have to make it easy for them. Let's start with the basics:

- **Get a solid, travel-and-security friendly laptop bag**. Since you said you'll be travelling with your laptop, your best bet is to keep it in a bag where it only needs

to be removed when you need to use it. You'll also want a bag that can keep your laptop safe from bumps and jolts so it survives the trip. Whether you prefer messengers or backpacks, make sure it has a well-padded laptop sleeve. Make sure your bag is travel-friendly, can be neatly collapsed or expanded depending on what's inside, and is comfortable to wear close to your body. You don't want your laptop bag to be so uncomfortable that you put it down every chance you get.

- **Keep your eyes on your gear**. If you're going to be working in a public (or even semi-public) environment, your best bet is to take your laptop with you when you have to move anywhere. Working from the library and need to go to the bathroom? Pack up your bag and take it with you. It sucks, but it sucks a lot less than losing a laptop with all of your data on it.
- **Always use your hotel's "Do Not Disturb" sign**. Half of the fun of being in a hotel is that someone else comes in and cleans up, but if you're working or need to leave your laptop in your room, put up the Do Not Disturb hanger on the outside of your door. Ideally, hotel staff will leave your room alone. The fewer people other than you in your room, the less likely your laptop will go missing. If you must leave without your laptop, use your hotel safe to store it (if it's large enough), but remember, hotel safes aren't all they're cracked up to be. Another alternative is to lock your laptop inside your suitcase, and make sure that's inside the wardrobe.
- **Buy a cable lock**. A cable lock won't stop determined thieves — they're easily cut, and many people don't apply them properly, but they can deter thieves in public or busy places.
- **Keep tabs on your laptop's location via software**. Services like Prey (which we've highlighted before for laptops), LoJack for Laptops, and even Apple's own Find My Mac will all help you locate a lost or stolen laptop if it does go missing. Accidents happen, and if you leave your computer in the back of a taxi, or it never makes it off the plane, or someone snatches it, you do have some resources to try and locate it, report it to the authorities, and recover it. These services work best when you sign up in advance, so make sure to register before your trip.

If you're worried about someone tampering with or opening up your laptop, that's a different issue. Such things are rare, but there's a lot someone could do just by plugging in a USB drive to your computer, or with a few minutes of physical access behind your back. You could go all out and grab some port covers for your laptop's ports, and then tape over them so they're inaccessible, but that also makes them inaccessible to you. Plus, as we learned from the glitter nail polish trick, techniques like that don't make your laptop tamper-*proof*, they just discourage people from tampering with them (so they're tamper-*resistant*) and they let you know when someone has tampered with it, so they're tamper-*evident*. The best protection against tampering is to keep your computer with you at all times and use a machine that isn't super-important to you.

Between these tips and some similar common sense (don't let other people use your laptop, don't use your laptop in sketchy places where you don't feel safe and comfortable working) you should be able to travel safely and work from your laptop without fear that it's going to randomly go missing.

Software Security

Next, it's time to make sure the data on your laptop is secure as well. Untrusted networks and insecure connections can make this difficult, and unfortunately if your laptop does wind up physically missing, you don't want it to take all of your precious data with it. Here's how you can use your laptop with confidence wherever you are, and make sure that data loss isn't the end of the world:

- **Back up everything before you leave**. If you're worried at all about data security when you travel, the first thing you should do before you leave is back up your data. Back up everything — take a full system image if your laptop, so you can re-image when you get home (or anytime along the way, if you make the image available to download remotely). At the very least, if something happens while you're travelling, the only information you'll have actually lost is anything you've created while you're on the road.
- **Cover the basics: Security software, strong password, lock screen, privacy-protecting browser tools**. When you're travelling you'll be working from strange places, possibly around strange people you may or may not trust. Make sure that you have security software installed, and that it's up to date. Similarly, make sure your system is protected by a strong password; you're not using an administrator account (and the admin account is either disabled or protected by a different strong password); that your computer is set to lock when idle or asleep; and that you lock it every time you have to leave it unattended. When using your browser — or any other web-connected tool — make sure you use SSL (HTTPS) and other secure protocols whenever possible. Check out these browser extensions to protect your privacy while you surf.
- **Use a VPN**. A reliable (and trustworthy) VPN is your best ally when it comes to making sure your data is secure anywhere you go. VPNs have their drawbacks, but if your security concern is the network you have to use — an airport or library, a hotel with a completely free and open network, or a food court — using a solid VPN can make all the difference. If you're travelling for work, your company may have a VPN you can use. If not, we have some suggestions.
- **Reinstall or re-image before you leave**. Once your data is backed up, consider running a slimmed down version of your operating system and any associated data while you're travelling. You may even be able to get away with using a live CD while you travel or booting into another operating system (like your favourite flavour of Linux) while you're working on the road. The best way to make sure you don't lose important data — or that someone doesn't get access to it while you're using free airport Wi-Fi — is to not have it on your machine at all. This also makes

you less vulnerable to spyware or other malware — if anything's detected, blow the system away and reinstall. You have nothing to lose. Travel light.

- **Wipe and re-image along the way, or at least after the trip**. Speaking of reinstalling if something goes wrong: if you're intent on using untrusted networks, you don't have a choice (the network won't play nice with your VPN, for example), or you just need the speed of a raw connection to whatever's available (see: journalists at CES right now), your next bet is to blow away your system on a regular basis and use web-based tools you can get to without installing more than you need. If most of the tools you use are on the web or available as portable apps you can slap on a USB drive or in Dropbox, you don't need to install anything, or keep any data locally if you don't have to. Install a fresh, patched up, clean OS, and just hit the road. At the very least, if you're worried about what you may have contracted while you're away, format and reinstall before you reconnect it to your home or office network when you return.
- **Encrypt your sensitive data, and keep it off your system if you can**. There was a time when encrypting sensitive information was difficult, but it's really not at this point. Tools such asTrueCrypt making encrypting local files, folders, and volumes easy. BoxCryptor can handle cloud storage like Dropbox. We've shown you how to encrypt Dropbox and encrypt local files or even your whole operating system. It's not hard, and it will make sure a thief or anyone else may get your machine, but not your data.

These methods range from the simple to the effort-intensive, so take them as you see fit, and judge them against the actual risk you think you and your data will face while you're away from home. Encryption is great, but it may be overkill if you don't have any data in the first place, and re-imaging your PC regularly while you travel can just waste time and effort if you're always working on trusted networks around people you know.

These tips should help you keep your laptop in one piece and in your possession, and your data safe from prying eyes or potential thieves while you travel and try to get some work done. Just make sure to keep security and safety in the back of your head, do a little planning, and exercise common sense, and you'll be fine. Have a safe trip!

Reference:

This was cross-posted from http://www.lifehacker.com.au/2015/10/how-can-i-make-sure-my-laptop-is-secure-while-i-travel-with-it/