access

/// ACCESS TECH /// 10-MINUTE GUIDE /// TO SAFER TRAVEL ///

October 2011

ACCESS TECH 10-MINUTE GUIDE TO SAFER TRAVEL

For more information, please contact:
soc@accessnow.org
PGP Key ID: 0xF08D380A

THE THREAT

Traveling exposes you, your devices, and your data to many risks. Laptops and other devices can fail or get stolen, lost, damaged, or impounded. Data in transmission from public access points such as Internet cafes and hotel wifi can be intercepted. Using untrusted systems may expose you to keyloggers and other attacks designed to capture information that should be kept secure.

In addition, when you are crossing any national border you have few if any rights to protest or refuse when a border control or customs officer wants to inspect any part of your luggage, including the data stored on your laptop, digital camera, recording device, or cellphone. Even in the US, despite the Fourth Amendment, a customs officer needs no "probable cause" or warrant to search your machine or impound it for further inspection.

THE RISKS

Will you be able to work if your machine and all its data is inaccessible? Will your co-workers, supporters, aides, allies, or donors be endangered if the data you're carrying is exposed to outside scrutiny? What will you do if someone who has intercepted or accessed your data uses what they've learned to impersonate you, potentially damaging your personal reputation and that of your project or organization and endangering those who innocently respond? A small amount of attention to security and safety can avoid all these consequences.

THE TOOLS

Many tools and practices are available to help you keep your data safe and secure while traveling at little or no cost. These include:

Data minimization – travel with as little data as possible.

Cryptography software – use (where legally permitted) on desktops, laptops, and some cellphones to encrypt email, files, and file systems.

Live CDs – run on public-access computers instead of the supplied operating system to ensure no data is kept and you are not tracked.

Temporary email addresses – use to ensure that your main email accounts are not compromised.

Tor – "The Onion Router," privacy technology designed to bypass censorship systems, secure data in transit, and protect against tracking and traffic analysis.

Cloud backup systems – use to store your data so you can travel with a minimum of data and/or

restore a machine that is inaccessible

USB sticks and other flash memory – use to keep important (encrypted!) data backed up in situations where online access is uncertain.

DATA MINIMIZATION

Data you are not carrying cannot be lost or stolen. Begin by considering what data you actually need while travelling and what can be left behind. Copy everything you do not need onto another computer or hard drive that will remain safe at your home or office. While you are doing this, also back up your sensitive data onto media such as CDs or DVDs and store them in a secure location separate from your main computer such as a small combination safe in an employee's residence.

Especially, ensure that you are not carrying any data that could be illegal in any of the countries you are traveling to. Potentially illegal data might include authorized copies of copyrighted material (such as music and video), pornography, and even innocent photographs of unclothed minors. If such material is found in a border search, your laptop could be confiscated.

One option used by some frequent travelers is to store either just their data (encypted) or an entire image of their system complete with software with a cloud service provider and travel with a bare-bones laptop. Once arrived at their destination, they then download the data and/or software, re-uploading it before departure. This set-up provides both data minimization and an accessible backup, although it limits what work you can do in transit.

ENCRYPTION

While it is always advisable to encrypt the data stored on your computer and communications devices, the import, export, and/or use of cryptography is illegal in sohme countries. Check the rules in the specific countries you will visit before traveling. In some cases you may need to apply for an import or export permit; in a few cases personal use may be banned entirely. You should also check on the legal situation with respect to handing over your private keys to law enforcement: in some countries you may go to jail if you refuse.

World map showing countries with import, use, or export controls: http://rechten.uvt.nl/koops/cryptolaw/cls-sum.htm

Detailed crypto import/use/export information by country: http://rechten.uvt.nl/koops/cryptolaw/cls2.htm

Some basic information on travel and encryption: http://www.princeton.edu/itsecurity/services/encryption/travel/

HARD DISK ENCRYPTION

Encryption is an important technique for ensuring that if someone gets hold of your laptop or other device and tries to access your data without your passphrase all they will see is a random pattern of 1s and 0s. Be aware, however, that using encryption makes recovery of your data harder if your hard drive suffers a drop, violent knock, or other form of abuse. The costs of this type of advanced data recovery are out of scope for most civil society organizations. Keeping good backups is essential.

PROTECTING CRYPTO KEYS

Probably the most valuable data on any device you carry with you will be your PGP/GPG private keys. You should pay particular attention to protecting them and the passphrase that unlocks them. This means not allowing such devices to be in the hands of third parties without supervision and not leaving the devices unattended when others have access to them. You may prefer not to keep your private keys on your devices at all. Instead you could keep them on a USB thumb drive that hangs around your neck and that you keep under your control at all times.

PUBLIC ACCESS

You will frequently have occasion to use public systems when traveling, whether these are computers provided in Internet cafes or other public areas or the wired or wireless networks in hotels, conference centers, and elsewhere. Each of these situations has its specific risks.

SHARED COMPUTERS

TRUSTED KEYBOARD

The most likely way your security will be thoroughly compromised is through logging into your accounts on a machine or keyboard that is not trusted. If you are not using your own laptop/ipad/iphone/android phone, then the keyboard is untrusted.

The particular danger is keyloggers, which capture everything you type into the computer for later inspection by attackers. These come in two types: hardware and software.

Hardware keyloggers, which are available for both PS/2 and USB form factors, are dongles inserted into the cable running between the keyboard and the computer You should check for these before using any keyboard that is not your own.

Another option is to travel with your own small USB keyboard that you can plug into untrusted computers without having to reboot.

UNTRUSTED SYSTEMS

Software keyloggers, which may operate at the kernel level, are a much more dangerous threat because it is so difficult to tell if they are present. For that reason, gaining any level of confidence in an untrusted computer is a daunting prospect.

The best solutions to this is a custom Live CD that you have prepared with your choice of operating system and the basic software you need. This lets you boot your own trusted operating system from the CD drive and bypass the untrusted computer's standard set-up entirely.

UNTRUSTED NETWORK ACCESS

The need to use untrusted connections to the Internet is a constant when traveling. These include hotel wired and wireless connections, Internet cafes, municipal and commercial hotspots, and so on. Rogue nodes in such networks may be able to perpetrate what are known as man-in-the-middle (MITM) attacks. These can capture the addresses of sites you visit and the addresses and contents of email. A rogue node can also divert your traffic from the genuine site you're trying to access to a dangerous fake.

Encryption — again — is the most important technology to ensure that data cannot be read by anyone who intercepts it in transit. A common solution is to use a virtual private network (VPN) connection to your home network, which sends all your Internet traffic through an encrypted tunnel to (and then possibly back out again from) your trusted system. SSH/SCP, which you run from a console on your computer, can also protect your connection to remote systems. HTTPS, which secures connections to specific Web sites, must be set up as an available protocol by the particular Web site you're using.

Regardless of which encrypted protocol you are using, pay attention if warnings pop up when you initiate a connection as such errors may well indicate a MITM attack. But their absence does not necessarily mean you're safe: some MITM attacks hijack sessions without triggering an error message. However, successful session hijacks will generally give attackers only a limited time in which to perpetrate damage, as they typically grant the attacker only the key for the current session.

TOR

Tor stands for "The Onion Router", and it is specifically designed to bypass censorship and provide anonymity for Web browsing and using other Internet resources in potentially hostile situations. It is therefore wise to use it when operating abroad, especially if you're inside a country where the incumbent regime is opposed to the actions of your NGO.

Because Tor slows down your connection, the ideal set-up is to have two browsers on your laptop. Use one with Tor for accessing sensitive information; use the other for general web surfing to non-sensitive information. However, be careful what you class as sensitive. Even apparently innocuous websites may actually give away a lot more about you and your intentions than you may at first realize. Seemingly mundane information such as your travel plans or making arrangements with people that tip off an eavesdropper that you will be out of your hotel room for a period of time can give away information that could be used to your disadvantage. If in doubt go via Tor.

ALTERNATIVE EMAIL ADDRESS

Because you will have to use untrusted connections and systems, it's a good idea to limit the consequences of an attack. One important tactic is to create a new, Web-based email address just for the trip that you will 'throw away' afterwards. Use this address for all non-sensitive communications while traveling so that if the account is compromised it will give the attacker no value beyond the end of your trip. Do not log into your regular email account until or unless you can be confident that the connection and computer are safe.

FURTHER ADVICE

WATCH OUT FOR SHOULDER SURFERS

Always be aware of who is in your immediate vicinity when you type in passwords, passphrases, and the PINs that protect credit cards and debit cards. Protecting against "shoulder surfers" who pick up your user IDs and passwords by watching from behind you or remotely (look for cameras) is the reason why today's operating systems replace the passwords you type in with a series of dots. But the same information can be picked up by watching your fingers on the keyboard, so be careful.

SET YOUR MACHINE TO LOCK AUTOMATICALLY WHEN UNATTENDED

Most operating systems provide a way of automatically locking the keyboard and display after the user has been inactive for a period of time. This is a good practice even though of course you intend never to leave your machine unattended. Similarly, you should set your computer to require your password at logon and whenever you resume from standby.

CHOOSING GOOD PASSWORDS/ PASSPHRASES

Passwords should be easy to type (because fast typing is harder to shoulder-surf), easy to remember, and hard to guess. While

it's generally acceptable to reuse passwords on sites of low importance (for example, the registration systems on news sites), you should choose unique passwords for sensitive sites — banking, financial services, your organization's network, your email — and the passphrase protecting your encryption keys. If you have used these passwords in insecure situations, you should change them afterwards when you're in a secure situation again.

For your passwords, do not use your name, your organization's name, any portion of your or your organization's street address, or the names of your pets, spouse, or children. Also do not use single words you can find in a dictionary of any language; these are easily cracked.

Most textbooks — and the rules on many Web sites — will tell you the safest passwords are those that have been randomly generated or that are at least eight characters long and include at least one capital letter and one number. Passwords created by these methods are hard to remember accurately and hard to type; many people, faced with having to remember a dozen of these, are forced to resort to writing them down, a very insecure practice.

A more usable strategy is to pick two unrelated words and concatenate them with one or more symbols or numbers. For your encryption key passphrase, create a memorable sentence; this will naturally have capitals, spaces, and punctuation and be very hard to guess.

HARD DRIVE ENCRYPTION BY PLATFORM

Software to encrypt your entire hard disk/s is available for all of the common operating systems.

MAC OS X

Full disk encryption is easiest on Mac OS X devices because it's built into the operating system and is even the default setting for new devices. In fact, you may have disk encryption activated without knowing it; when you log onto your Mac your account password is the 'secret' that unlocks the private keys that are used to decrypt your hard drive.

To check if disk encryption is on or to turn it on for Mac OS X laptops, go to 'System Preferences' --> 'Personal' --> 'Security' --> 'FileVault'. On that dialog box it will tell you if FileVault is 'on' or 'off' and there will be a button to either 'Turn on FileVault' or 'Turn off FileVault' depending on the current status of this feature.

MICROSOFT WINDOWS

The Ulitmate and Enterprise editions of Vista and Windows 7 have full hard disk encryption capability available via the included BitLocker Drive Encryption system. A step-by-step guide for Windows 7 can be found on Microsoft's Technet: http://technet.microsoft.com/en-us/library/dd835565(WS.10).aspx

For versions of Microsoft Windows do not ship with BitLocker, such as XP and the home edictions of Vista and 7, there are many options including several free, open source full-disk encryption software applications. We recommend Truecrypt: http://www.truecrypt.org. Truecrypt is simple to install and use, and offers many options for encrypting all or part of your hard drive, including hiding the encrypted portion.

LINUX

Truecrypt and many other open source options are available for full hard disk encryption on all distributions of the Linux operating system.

Access is an international NGO that promotes open access to the internet as a means to free, full, and safe participation in society and the realization of human rights. Founded in the wake of the 2009 Iranian post-election crackdown, Access works to build the technical capacity of digital activists and civil society groups, provide thought leadership and pragmatic policy recommendations to actors in the private and public sectors, and mobilize its global movement of citizens to campaign for digital rights.

For more information, please visit **https://www.accessnow.org** or email **soc@accessnow.org (PGP Key ID: 0xF08D380A)**