Online Security for Independent Media and Civil Society Activists

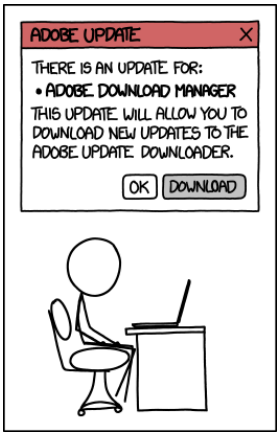
A white paper for SIDA's October 2010 "Exile Media" conference

Eric S Johnson
(updated 13 Oct 2013)

For activists who make it a priority to deliver news to citizens of countries which try to control the information to which their citizens have access, the internet has provided massive new opportunities. But those countries' governments also realise ICTs' potential and implement countermeasures to impede the delivery of independent news via the internet. This paper covers what exile media can or should do to protect itself, addressing three categories of issues:

- common computer security precautions,
- defense against targeted attacks, and
- circumventing cybercensorship,

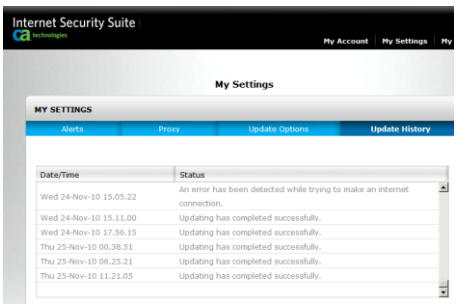
with a final note about overkill (aka FUD: fear, uncertainty, doubt). For each of the issues mentioned below, specific examples from within the human rights or freedom of expression world can be provided where non-observance was catastrophic, but most of those who suffered problems would rather not be named. [NB Snowdengate changed little or nothing about these recommendations.]



Common computer security: The best defense is a good … (aka "lock your doors")

The main threats to exile media's successful use of ICTs—and solutions—are the same as for any other computer user:

1) Ensure all ***software automatically patches itself regularly*** against newly-discovered security flaws (e.g. to maintain up-to-date SSL certificate revocation lists). As with antivirus software, this may cost something; e.g. with Microsoft (Windows and Office), it may require your software be legally purchased (or use the WSUS Offline Update tool, which helps in low-bandwidth environments). Firefox, Chrome, Adobe Acrobat Reader and Flash player, iTunes+QuickTime, Skype (and other IM clients), and Java VM should update themselves (or prompt you to install updates), but verify from time to time. MBSA's scan is more complete than Windows Update. The free Windows Secunia PSI, Ninite or Mac OS MacUpdate patch managers tell you about needed updates and ease installation; IBM's BigFix is for-fee. Always use the newest (e.g. 64-bit Windows' ASLR is stronger than x86's). Keep your smartphone's operating system (Android, iOS) updated (i.e. don't jailbreak them—doing so reduces security). Fully reboot at least weekly to ensure boot-triggered update checks and installs are executed. (~USD100/computer/yr to license software)
2) ***Use a good antivirus*** on all computers—one which automatically updates its virus-fighting capabilities (e.g. TMIS, McAfee, NIS, Avira, Kaspersky, CA, Immunet (ClamAV), F-Secure, Avast, AVG, MS Security Essentials, BluePoint (the latter's the most restrictive, since it uses a whitelist), but use only one). An antivirus program in a "security suite" will come with a firewall / intrusion protection system (the ones built in to Windows 7+ and Mac OS 10.7+ are good, but a third-party one adds outgoing-connection control), anti-spam, and malware protection. If you feel that more is better, consider adding Anti-malware, ThreatFire, or Ad-Aware (all free). Ensuring Windows' data execution prevention is on (most thoroughly, through EMET configured explicitly to include all software which parses untrusted files from the internet) provides an additional security boost. (ClamAV, MSE, AVG, Avast free; others ~USD40/computer/year)



3) Avoid falling for phishing lures and malware (can't say it too often!):
   a. ***Don't open attachments*** (from an unknown source) to, ***or click on links*** in, e-mail messages—they might result in stolen documents, giving botnets (such as those tracked by ShadowServer) control over your computer, or allowing government law enforcement agencies remote access to your files (using e.g. offensive security products such as FinFisher, HackingTeam, Vupen). The most devastating cyberattacks tend to start with spear-phishing: the bad guy sends you malware-laced e-mails which look as if they came from someone you know and trust (usually with a ZIP attached). If you must open an attached file, upload it

to and open it in Google Drive, so it runs in Google's sandbox (and can't hurt you); or at least, first scan it with Jotti or VirusTotal. If you think you've received a spear-phishing e-mail, share it with someone like the Internet Freedom Project (which can use e.g. the Norman Malware Analyzer G2, and can collate data with that from many analogous attacks) to get confirmation.

b. ***Never enter your password into a site accessed from a link in an e-mail***; when your receive from your bank "your statement's ready to view," type the URL into your browser (or use a shortcut from your "favourites"). (The URL in the hyperlink might be fake, in which case you'll be clickjacked; you can't tell the difference!)

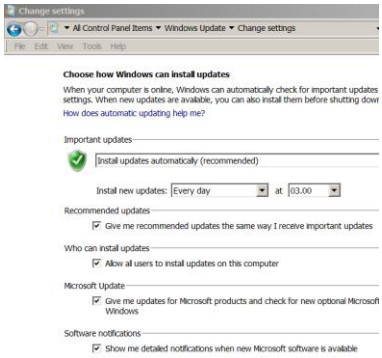
c. ***Never provide your online account login credentials to third parties*** such as that site with "please enter your [e.g. Gmail] account login and password so we can provide you with X" or the phone call offering to help with your virus infection. Most such offers aren't legit. If you respond, at best your account'll be used to spam everyone in your address book; or, someone will stealthily monitor your account and/or use it to trick your friends into revealing important information; or, worse, your account or computer will be locked until you pay a ransom.

d. ***Don't click on links sent to you from Facebook, Skype or Twitter friends/feeds***—you might be likejacked and/or catch malware, especially something targeted (e.g. at independent thinkers in Syria or Russia).

e. ***Don't install crapware*** such as browser toolbars (especially originating in a potentially hostile country, e.g. China's Qihoo), software crackers, or third-party utilities which promise to "speed up your computer."

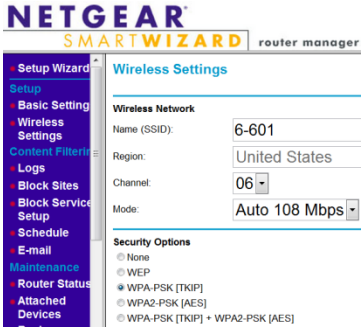
Check your e-mail accounts' settings/options monthly to ensure there's no unexplained forwarding. Deploy the free Simple Phishing Toolkit to test your employees; train the 15% who will "fall for it" how to avoid being phished.

4) ***Retain physical control/possession*** of all your devices. Never enter a password into a computer running an OS you don't control (e.g. a cybercafé's), and never lose control of your own notebook and mobile phone: a rootkit (= total compromise) can be installed in seconds. Set your computer to require a boot password; ensure your screensaver automatically locks your computer after short inactivity; if you part from your computer while it's on, lock it (Windows' flag-L, Mac OS's ctrl-shift-eject). (Don't leave even a full-hard-drive-encrypted notebook alone in e.g. your hotel room—someone could open it up and install a hardware keylogger.)



5) ***Back up*** every other week, protecting against loss due to attack, loss, or technical failure. The most secure backup is (online) Tarsnap for *nix. Other OSes have simple programs built in (Win 7's Windows Backup, Win8's File History, Mac OS's Time Machine) to back up your data (i.e. in Windows 7+, c:\users\[your-name]\). Third-party specialised backup programs automate the process (e.g. the open-source Cobian, AllwaySync or Acronis for Windows, Retrospect for the Mac). Backups must be encrypted too (either the backup file(s) or the medium). Keep an off-site copy so if your house burns, not all's lost. E.g. use a secure (client-side-encrypted) online ("cloud") service such as CrashPlan, SpiderOak, SamsBox, Mozy, BackBlaze, or wuala (select "use private password" (or key); or encrypt your outgoing data with BoxCryptor, for Dropbox, or CipherDocs / SecureDocs / Syncdocs for Google Docs/Drive)—but some free services delete after x (e.g. 30) days of non-use. Also back up your site (it will eventually be hacked)—including CMS database(s) (not just static pages)—using e.g. cloud-based CodeGuard. Back up your mobile's contact list. (USD20/user for a high-capacity USB thumbdrive)

6) ***Use strong passwords; set password recovery mechanisms***. Don't use the same password as everyone else, or simply a name or word (otherwise Cain & Able can guess it). Passwords must be at least 10 characters (otherwise vulnerable to brute-force-crackers HashCat, TrueCrack). When signing up for an online service, provide backup contact information and (hard-to-guess!) answers to security questions to authenticate you in case control of your account is lost. (Don't daisy-chain your accounts, else if one's compromised, all others are.) If you lose control, contact RSF, HRW, or Internews (all affiliated with the Global Network Intiative, thus plugged in to large service providers) to recover it. Don't reuse passwords across services. Try to avoid using your e-mail address as your login. If your whole-hard-disk encryption is on, use LastPass, Keepass, or 1password to make and remember strong passwords. ***Don't share a password*** with co-workers or paste it on a PostIt on your monitor! If available (e.g. via Gmail, Dropbox, Apple), turn on two-factor authentication (then customize it with app-specific passwords (e.g. for Gmail and Facebook)).



7) ***Secure your office and home wi-fi access points*** (APs)**.** Change the manufacturer-set password for your AP's control panel and wifi encryption. Use WPA2-AES for encryption, since the older WEP is insecure: sniffing open wi-fi's a simple way for snoops to access your entire digital life. Turn off WPS, since it provides attackers a "hole" through which to enter. Audit your network with NetStumbler or inSSIDer.

8) ***Don't transmit personal data via unpassworded wifi hotspots*** except encryptedly—use an HSTS-compliant browser

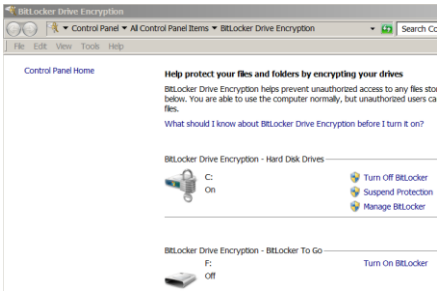
(Chrome, Firefox, Opera; not IE, Safari), HTTPS Everywhere, or a virtual private network (VPN). Otherwise, others in Starbucks could use DriftNet to see what you're downloading, or FireSheep (or DroidSheep on a mobile) to sidejack your Facebook account to social-engineer her way into the confidence of your friends (unless you use the *non-default* encrypted access to Twitter, Google, and LinkedIn; set each's preferences to "HTTPS only" (the default for Facebook users)), or Wireshark to see everything.

9) ***Secure your real-time online communications*** by using (on both ends!) instant-messaging (IM) and VoIP solutions which are *encrypted*. The real Skype (not the cybercensorship- and cybersurveillance-laden Chinese TOM Skype, and not the business version, which a network administrator can control) is; so are Gchat (IM via your Gmail webmail interface) and FaceTime; or apply open-source encryption over otherwise-unencrypted networks—ICQ, AIM, MSN, Y!, Gtalk, Facebook Chat, or iChat (the latter three running on XMPP): OTR on top of a universal IM client (IM+, Pidgin, Miranda, Jitsi for Win; Adium for Mac) or XMPP-only Psi (using OpenPGP). For mobiles, CryptTweet runs under Python (on Win Phone, Linux, Android, and iOS). VoIP via Zfone, (for-fee) Silent Circle (using ZRTP), and Blink (using SIP/SRTP) are encrypted—but also source-code-published so peer-reviewed and therefore more trustworthy. Skype-like Viber and ooVoo, and group "open-mic" chat group software clients Zello and Raidcall, aren't encrypted. If your IM or VoIP software doesn't say it's encrypted, it probably isn't (e.g. QQ, WeChat, Pfingo).
10) ***Don't forget "conventional" surveillance of computer use*** (opsec). In a public place, be aware of the person sitting next to you in the cafe, the camera on the wall recording what's on your screen, the "conventional" bug recording your Skype/VoIP conversations, etc. Take care who you tell what you do. And worry about the ***cybersecurity of whomever you're communicating with***!

Targeted attacks: Higher—or hired—technology (aka "manage your risk")

Attacks can come in many forms; defending against all of them is impossible, but there are steps to take—some easier, some more sophisticated.

11) Internet traffic is massive and dispersed; online surveillance isn't trivial. A hostile's more likely to try to get your hard drive (HDD/SSD). Ensure all computers—especially notebooks, more likely to be lost or stolen—***use whole-hard-disk encryption*** (WDE) (the "Windows login password" without WDE can be circumvented by a USD20 USB-to-SATA bridge). Ensure your HDD has hardware encryption (e.g. Digisafe DiskCrypt, Crypto SSD), or use software encryption: Windows 8 Pro includes easy-to-use BitLocker (Windows 7 Ultimate's implementation requires TPM 1.2, a chip in most business-class notebooks (except in Russia and China, where TPM's theoretically banned)) and Mac OS 10.7 (Lion) and later includes FileVault 2 (incompatible with PGP Desktop); LUKS via dm-crypt (built in to the Ubuntu distro beginning with 12.10) serves Linux users. Free (if harder-to-use) WDE solutions include multi-platform TrueCrypt, Windows-only Compusec. For-fee programs include PGP WDE or Check Point FDE for Windows, SecureDoc or SafeGuard for Mac OS X. (In all cases, either disable **all** DMA-compliant ports (including Firewire, PCIe, USB3, Thunderbolt, PCMCIA, ExpressCard, and Ultrabay), or use YoNTMA to help prevent a thief from using Passware or Inception to bypass your disk's encryption *when your computer's not entirely off*.) Any of the above can also be used to encrypt removable media such as thumbdrives, although the optimal thumbdrive solution is an IronKey, which has encryption built in. (Creating an encrypted vault for your data files (Windows' EFS, Apple's FileVault, Linux's EncryptFs) isn't as good: computer use leaves much metadata which a forensics specialist can discover, even without access to your core data.) If your HDD's encrypted, programs like CCleaner or AShampoo's WinOptimizer (which empty temporary data caches and more thoroughly erase files) are superfluous. (~USD90 to upgrade Windows; 1G IronKey D200, USD59)

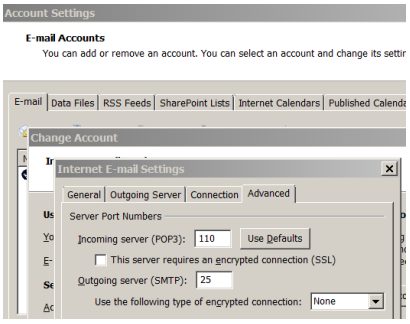


12) To defend against online snooping, ***encrypt your computer's communication with your mail server***. Gmail is the only major free webmail provider which encrypts (via HTTPS) **all** access (so do some smaller services such as the US's Riseup, the IL SAFe-mail, the CA Hushmail, and the DE GMX); the US's Hotmail, Yahoo!, and AOL, the AU/US/NO FastMail, and the RU Yandex allow HTTPS webmail access but you need to turn it on; if you use others, e.g. Live.com, Mail.ru, 163.com, qq.com, rediff.com, assume your communications **aren't secure**. (All of the Big Three webmail providers also allow encrypted access via POP3/IMAP, although with Yahoo! it requires upgrading to its USD2/mo Plus.) To encrypt the transmission of mail from within a mail client, you need to dig into its settings:
    a. in Outlook 2010 or 2013, "file -> account settings -> account settings -> [select your account] -> change -> more settings -> advanced," both *enable SSL* and *enter in your mail server's SSL port* (usually 465 for sending (SMTP) and 995 for receiving (POP3/IMAP)). Indicate (on the "outgoing server" tab) that "my outgoing server requires authentication: use the same settings as my incoming mail server."
    b. Thunderbird is more likely to automatically configure SSL use, but if it doesn't, the "tools -> account settings ->

server settings / outgoing server -> edit" allows manual configuration; in addition to setting server name and port, don't forget to click "use name and password."

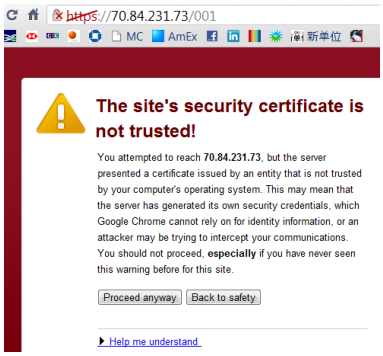
Some hosting companies will also require you to use a different server name (than your usual one) and/or a non-standard port (e.g. 587/993) for sending and/or receiving encryptedly. Be sure to use "require SSL/TLS," not STARTTLS (which would be vulnerable to an SSLStrip-like MITM attack). (No cost.)

13) Defend against attempts to listen to even your encrypted (HTTPS) web traffic.
    a. Be sure all of your devices (computers, phones) in "hostile" countries are using an ***OS and software which originated outside that country*** (one from a relatively free country?), e.g. buy your notebook (with pre-installed OS) abroad. Otherwise the OS may have had inserted into it (at install time) a "trusted root certificate" which would enable the government's gateway devices (e.g. from Blue Coat, Palo Alto, Packet Forensics, Narus, Cisco, Huawei, or ZTE) to conduct man-in-the-middle (MITM) interception of your encrypted (SSL) traffic. Or it might have malware pre-loaded. If you live in China, tell your browser not to trust the CNNIC CA (or, use a Firefox add-in such as CertPatrol or CertLock).
    b. When your browser warns you about a "bad certificate" (which is what would be created by a simple MITM attack using Burp Suite or Fiddler), assume communication with that site isn't secure.
    c. Use Chrome (the safest browser, because it has Gmail's certs pinned), or Firefox; don't use third-party browsers like Qihoo 360, which may have backdoors built in.



14) ***Create backup*** ("burner") ***Windows, Gmail, and Facebook accounts*** and populate them with *some* legitimate data so you can "give away" access to them when you're threatened or arrested.

15) Establish a relationship with the ***management of the company(s) hosting your domain and your site*** (and ensure your technical and administrative contact information for both of them is up-to-date) for three reasons:
    a. In a social engineering scenario, an attacker impersonates you, convinces your hosting company to provide access to your domain or site, gains control, and alters or deletes your content. You would like to ensure that your hosting company has a personal relationship with you (and a lock-tight identity authentication procedure), so that they will verify third-party attempts to be given access your site's control panel before allowing them to proceed.
    b. In a hacking scenario, an attacker takes advantage of vulnerabilities in the software on the server used to host and deliver your content to visitors. You want to ensure your hosting company keeps its software—most importantly, your CMS (SPIP, WordPress, Joomla, Drupal) *and its plug-ins*—up-to-date with whatever patches fix the most-recently-discovered bugs (although it's more likely you'll have to do this updating yourself). (Make sure your domain's locked and its ownership anonymised.)
    c. In a betrayal scenario, your hosting company's interests or presence in a certain country makes it susceptible to pressure from that country's government to impede your site's operation or provide information to LEAs. Use providers (of DNS registration, of web site hosting, of e-mail hosting) unlikely to betray you to the government you consider your main adversary—perhaps ones which operate only in the US or EU.



In any of these cases, if something happens, you want to be prepared to quickly find someone at your hosting provider with whom to talk, to provoke quick mitigation action. ISPs known to have been friendly in the past include PRQ in Sweden, Shinjiru in Malaysia, OVH in France, Greenhost in the Netherlands, WebArchitects in Iceland, Positive Internet in the US, and (for extra-security WordPress hosting) WP Engine in the US (also, Deflect has rated VPSs for their DDoS-absorbing purposes). (~USD50/month for hosting, instead of USD10/mo)

16) ***Secure your organisation's server*** (this is hard). The best defence against advanced persistent threats (APTs, aka hackers targeting you) is to keep your server software up-to-date (perhaps use Pakiti). Harden your server software using CIS's app-specific benchmark tools. Use a vulnerability scanning service like the free CyberSpark (or regularly run pen-testing software such as free Metaspolit, Nexpose, Nmap, Arachni, Nikto or for-fee Tenable Nessus, Netsparker, Acunetix, StopTheHacker) to monitor your site's performance and security, then act upon easily-detected weaknesses. Ensure user databases (e.g. login credentials, or your mailing list's e-mail addresses) are encrypted and/or hash-salted (with multiple iterations) using bcrypt or SHA-3, not SHA-1 or MD5; ensure databases (such as MySQL and Oracle) are audited and/or "locked down." Don't keep logfiles with IP addresses (hackers could ID your visitors). If you allow logins, set a lockout or timeout to prevent brute-force cracking; if you have multiple Windows servers, enable EPA to defend against forwarding attacks; use fail2ban and iptables to block access from attacking IPs. Use an intrusion detection system (IDS) like Trisul, NTV, TippingPoint, or Security Onion to monitor your company

network gateway's flows. Analyze log files periodically to identify anomalies. Set your site to provide service by HTTPS (using e.g. a free server cert from StartSSL); verify it with Qualys' test. Consider implementing DNSSEC; verify it with Verisign's testing tool. If you code, guard against the OWASP top 10 web application development security mistakes, and audit for security.

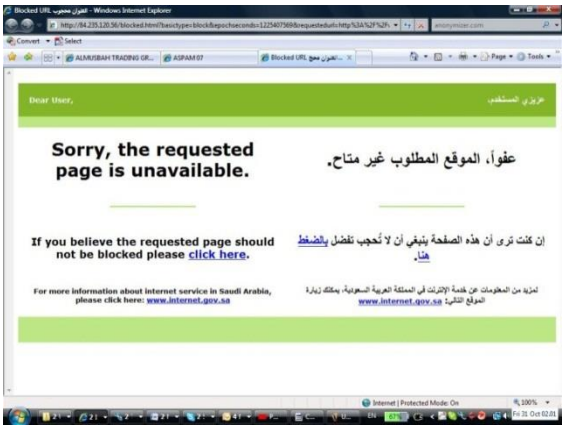
17) ***Secure your office network***. Control who uses it, and for what, with a network access control solution like PacketFence. Turn on DNS logging and regularly mine your DNS logs to look for evidence of penetration or malicious activity. Be a good citizen: don't leave open SMTP relays or DNS resolvers (they can easily be abused to hurt others).
18) Acquire ***hardened hosting***, to fend off distributed denial-of-service (DDoS) attacks which would prevent your constituency's access to your site. (DDoS results when your opponent hires—for as little as USD50/day—the services of a botnet (thousands of PCs) to create an excessive amount of access to your content, thus overwhelming your site's ability to respond and making it inaccessible to legitimate visitors.) There are several approaches, individually or in combination:
    a. Use a hosting service (e.g. blogger.com) located on an ISP with lots of bandwidth (at least two upstream providers, at least 1 gbps each), which increases the likelihood that the resources to deal with DDoS attacks are available.
    b. Buy DDoS protection from a third party which specialises in repulsing online attacks. Media Freedom's VirtualRoad (set up by the Danish media support organisation IMS), PRQ, RIMU, Qrator, and ServerOrigin make available services starting at as low as USD150/mo (although the onboarding fee can be more); Arbor Networks, Nexusguard, Staminus, Prolexic, Gigenet, BlockDos offer higher-end commercial-grade on- and off-site protection, but their prices are higher (~USD500/mo per 1-gbps/100K-pps of protection).
    c. Mirror your site in several locations around the world, and implement anycast in BGP to differentially advertise your IP address depending on who's visiting your site: visitors from different parts of the world will see different mirrors. An attacker's firepower is distributed across more than one site (therefore blunted); if the DDoS attack originates from a limited subnet, it'll take down your mirror "closest" to the attack source, but other mirrors will remain operational. (Cheap, but technically non-trivial.)
    d. Outsource the mirroring to a content delivery network (CDN) such as the free/low-cost CloudFlare and Incapsula or for-fee Akamai, Limelight, or EdgeCast.

    A stopgap measure to mitigate an attack is to simplify your site's home page so it doesn't load elements from a CMS (which heavily loads a server). The simplest landing page starts with a CAPTCHA challenge; only humans can pass through to your (presumably much more content-heavy, and therefore demanding of server resources) home page. Team Cymru and eQuality's Deflect (at no cost) help rights defenders protect themselves against a DDoS attack. Also, harden your DNS hosting (e.g. via HotPotato, UltraDNS, or DNSPod). For a more detail on activists' DDoS problems, see Berkman's study. For more detail on how to defend against a DDOS attack, see Access's and EFF's guides.
19) ***Upload files*** (e.g. you're a radio journalist) ***encryptedly*** using HTTP**S**, **S**FTP, **S**CP (WinSCP supports both of the latter two), or rsync via an SSH tunnel (ideally requiring you to have a (passphrased) cert (authorized private key) instead of the more-usual login/password combination). (FTP and RCP aren't encrypted.)
20) ***Split access to your site and/or blog into two***: a public one for visitors and a private one (secret domain; encrypted-only access) to make it impossible for attackers to even try to break in to your cPanel / CMS; constrain cPanel access to via SSH; yet more secure, use a Tor hidden service.
21) ***Expect all use of telephones*** (landline, mobile, SMS) to communicate with people in "hostile" countries ***to be under surveillance*** by the phone company (using e.g. Polaris' Altus Mobile)—intercepting calls and/or tracking who's in touch with whom is trivial. Mobiles can be remotely turned by the phone company (an emergency warning feature), which makes it easy to be geolocated. If specialised software has been installed, a mobile's microphone could be turned on remotely, regardless of whether the phone's on. Even without telco assistance, nearby mobile use can be intercepted by anyone with an IMSI catcher. Any time a mobile's on, its location is being recorded by the telco and, possibly, by the phone itself (for location-dependent services' use)—regardless of whether the phone is GPS-capable and/or GPS is enabled. Mobiles run on (Nokia) Symbian, Android, (Apple) iOS, BlackBerry OS (BBOS), and Windows Phone; no app provides universal SMS cross-platform encrypted communications, but *Skype IM + VoIP clients are available for all smartphone OSes.* Gibberbot +ChatSecure provide OTR-compliant encrypted IM for Android & iOS users; iMessage is end-to-end encrypted for iOS users. TextSecure provides encrypted SMS for Android. BBM (on the BBOS) is encrypted but RIM (which owns BB) has been known to give back-door access to LEAs. Never use an airport charger (which could be juice-jacking you—sucking data off your phone without your knowledge).
22) ***Use caution installing smartphone apps***—particularly if they ask for permissions (send/receiving SMSs, calling (which leads to toll fraud), contacts, location)—Lookout (for Android, iOS) can tell you which apps access which information. Some rack up illicit charges or harvest data for phishing. Android antivirus programs don't work well.
23) ***Satellite phones*** (Thuraya, Iridium, Inmarsat (R)BGAN) ***have GPS technology*** and tell their "mother service" where

they are; to preserve your location's confidentiality, turn off your satphone's GPS, or hack it to provide false information. Hostile governments can (using technology from e.g. Shoghi, TS2, Toplink Pacific, or Delma MMS) even intercept some satphone communications, including reading whatever self-locating data the phones are sending. (Iridium's safest because it can operate without its GPS.)

24) The location cache, call log (transactional details), and contact list on your ***mobile phone and tablet are a primary target of security services***. Change your default voicemail password (if the one set by the phone company is stock, it can be guessed, then monitored). On your smartphone, require the entry of a strong password before every use (on an iPhone/iPad, disable "simple passcode" to enter a longer one) and set an auto-lock timeout (so that after e.g. 1 minute, your phone locks); dumbphones and featurephones don't offer this. Regardless, a police forensics expert could use CelleBrite to extract SIM data, so turn on the "whole hard disk encryption" (built in to Android 4+ and BBOS 4.2+) that is much more secure—and disable USB debugging to close a "back door." The Data Protection functionality in Apple's iOS 4+ (on iPhones and iPads) encrypts only data using its API—e.g. the iOS mail program, but not most other apps (e.g. address book, SMSs, photos, Facebook …). Assume all Bluetooth communications are insecure.
25) ***Use caution with social network sites*** (SNSs) such as Facebook, LinkedIn, Twitter, Renren, Kaixin001, Odnoklassniki, Vkontakte, or Orkut. Users' presumption of confidentiality regarding the data posted on SNSs is often not justified: auxiliary applications share SNS users' friends' data, SNSes change privacy policies. Ensure you're okay with your SNS's privacy settings' permissiveness (e.g. you can choose to opt out of LinkedIn's social advertising). Assume everything on an SNS is public: lists of friends, postings, profile data, even IM content (e.g. Facebook Chat). Online data is persistent, e.g. once you've posted it, it'll likely remain there (or somewhere, i.e. the Wayback Machine) forever. At the very least, ensure your SNS access is encrypted (e.g. turn on Facebook's "use SSL" option).
26) ***Minimize online availability of your private information*** to reduce your chances of being socialed. Use a privacy-shielding service for your domain name registration. Google your e-mail address and phone number (together) to find—and take down—sources of data hackers can use to impersonate you. Don't use (or allow others to use) "I'm on vacation" auto-replies which reveal names, titles, and contact information of co-workrs. To monitor what Google knows about you, check your dashboard, edit your profile, and opt in to its monthly report about how you're tracked.
27) ***Be aware of photos' metadata*** when posting pictures online. Many cameras, especially smartphones', embed location information which can be used to trace the picture's shooter. Even older cameras embed their serial number; a quick search might discover other pictures with the same s/n—again, possibly compromising the shooter's identity. (Ditto screenshots from a computer's screen.) Use a metadata scrubber.
28) ***Dispose of storage smartly.*** After you toss your old unencrypted hard drives and/or USB thumbdrives, a dumpster-diver could easily find your data and compromise your security (ditto for selling old hardware). (Similarly, if you find a USB thumbdrive in a parking lot, use care; it could be a honeypot (loaded with malware).) (Don't forget to shred printouts of sensitive documents—trash paper can easily be recovered by the wrong person.)
29) ***Don't store data in the cloud*** unless you have the only key. A Dropbox hack or a court order with little judicial review could result in your information's compromise. (Per the US Justice Department, read mail in your online mailbox falls outside of US Stored Communications Act privacy protections.)

Cybercensorship: Help the mouse frustrate the cat



China's great firewall is only the best-known cybercensorship effort. Eleven countries seriously filter their domestic internet to limit access to politically sensitive content: Bahrain, China, Cuba, Eritrea, Ethiopia, Iran, Saudi Arabia, Syria, Turkmenistan, Uzbekistan, and Vietnam (MY, TN, and YE have stopped). (Another 25 countries' 'net censorship is mostly targeted at other content: sex, hate speech, religion, gaming, piracy; North Korea lacks public internet.) Cybercensorship starts with blocking domains, e.g. browsers' requests to return any content from facebook.com (or its underlying IP address(es)) are thwarted. Some countries (e.g. Ethiopia) conduct URL keyword searches, blocking requests containing phrases on the (secret) blacklist. Some firewalls (e.g. Syria) implement deep packet inspection (DPI), blocking (or altering) web traffic if certain words or protocols are found in packets' contents. Some countries replace a blocked site's page with an explanation; others hope users will attribute "page not found" errors to the internet's flakiness. (More insidious (e.g. Belarus) is "shaping," when access to certain sites is slowed, making netizens think the problem's at the provider's end, or punishing (e.g. in China): an attempt to view blocked content results in your international internet access being cut for about five minutes.)

There is no one-stop solution to figure out what's cybercensored; most countries' firewalls don't publish lists of filtered URLs. The crowdsourced Herdict and RespectMyNet offer users the opportunity to report content they believe

blocked or throttled. The cybercircumvention tool Alkasir uses a similar method but actually verifies all reports, then split-tunnels its users' traffic (proxying only what's known to be blocked) based on its lists. The P2P Lantern works similarly but allows users to edit the whitelist. The VPN Astrill does the same, but only for China (and doesn't make public its whitelist); the FireFox add-on AutoProxy does something similar, but only as a "simple web proxy" rather than a VPN; autoDDvpn can add this functionality (only for China) to a wifi AP. The Open Internet Project has created a series of pages listing the blocked content it believes is most popular for each country (e.g. Iran), and GreatFirewall.biz tracks what's blocked in China, in real time. A user inside a cybercensoring country can deploy Citizen Lab's (private) rTurtle, Astrubal's (public) 403 Checker, or OONI resources to verify whether a predefined list of URLs are blocked. UC-Berkeley's Netalyzr tests an individual's internet connectivity to identify abnormalities, intermediate proxies, and port blocking.

All cybercensorship-busting solutions "proxy" blocked content through an intermediate server which isn't blocked (until it is). A cottage industry helps cybercensored internet users find and use proxies. A netizen's most reliable and complete solution is use of a for-fee PPTP-, L2TP-, or OpenVPN-based VPN subscription for about USD5/mo; a recent report catalogued over 100 VPN providers, of which WiTopia, SmartVPN, StrongVPN, and 12vpn are among the larger ones (most are multi-platform).

But internauts without a Western credit card or PayPal account must find other options. The simplest are the thousands of (HTTP, SOCKS; PHP, CGI, Glype, Zelune) free browser proxies which can be found via a Google search; most are ad-supported. But browser proxies usually operate unencryptedly, are unable to handle sophisticated JavaScript (of which Facebook and YouTube make liberal use), and are themselves easily blocked. Psiphon is a special browser proxy, written to accommodate the most-blocked sites' content, and harder to block since its servers' addresses are not public (new users are invited in by existing users). Downloadable, free proxy clients are also popular: Hotspot Shield, Freegate, UltraSurf, Tor, and Puff (aka Simurgh) dominate the field (some can be run off a thumbdrive); smaller ones include Your Freedom, Alkasir, JonDonym, and Gpass; check your download's fingerprint before installing. (Freegate serves only China-source users.) The newest for-mobiles versions of Opera, Chrome, and Firefox use a (SPDY-like) protocol built to improve speed by compressing content via a browser-provided proxy server—thus circumventing a firewall, too. Or, ask friend in the uncensored world to run the Scotty gateway, to which you can create a secure tunnel.

30) ***Increase your anonymity*** by using any cybercircumvention solution to prevent your ISP from logging what sites you're visiting (defending against Palantir's data mining, but also preventing governments from tracking who posted what, on which blog, when). Tor's crowdsourced mesh-network-like design offers a virtual guarantee of anonymity, but slows down internet usage. For maximum protection (and to foil DNS poisoning, yet another cybercensorship mechanism used by e.g. Kazakhstan) use an alternative DNS service such Google DNS or OpenDNS. Use DNSCrypt to encrypt your DNS queries. "Privacy-guard" your domain name registration, hosting plan ownership, and server IP information, and beware using third-party embed tools such as Google Analytics which can be traced to you.
31) Help ***provide consumers with cybercircumvention*** they need to access your (blocked) content as well as to foil their governments' filtration attempts. Determine what sources of advice and software are not blocked from within your target population's country and publish URLs of services such as Sesawe, Technical ways to get around censorship, the 12 pm Tutorials, or Everyone's Guide to Bypassing Internet Censorship. Distribute to your cybercensored friends a private Psiphon server, or set up a private CGIProxy proxy server. Recommend software based on field tests (since the cybercensors in e.g. China and Iran successfully block the use of some proxy clients—until the proxy clients change servers). No one's ever been punished for *per se* circumventing their country's internet censorship. (No cost)
32) If you secure additional funding to support the battle against cybercensorship, consider ***financing the provisioning of additional free-for-the-user circumvention capabilities*** (more bandwidth, or even a branded circumvention solution) targeting your users. Any of the above proxy client providers would be glad to help. (~USD1/user/mo)
33) Explore alternative ways to deliver your content to cybercensored netizens, e.g. enable ***receiving news by e-mail*** via a mailing list. Use a professional mailing list management service such as iContact, Constant Contact, GetResponse, or MailChimp to preserve control over your list's confidentiality, maximise delivery rates, and ease list maintenance. Make sure users can subscribe by e-mail, to avoid a potential web censorship choke-point. (~USD10/mo)

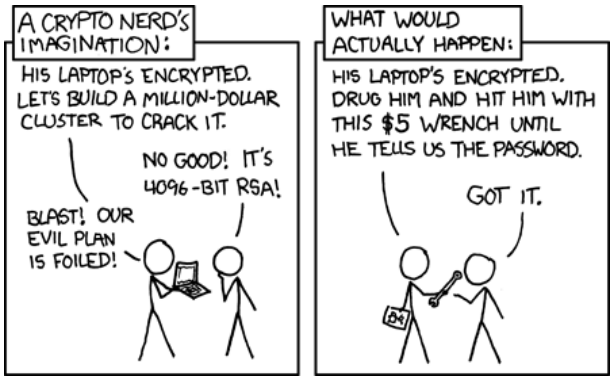
Too-serious security

All of the above advice is directed at people with a *moderate* level of security concern. If your demands are *high*—you're a diplomat with state secrets, or a businessman with trade secrets, or you activities mean you're seriously likely to be subject to a "rubber hose" threat—then your needs are different, perhaps even bulletproof. You may want to travel without any data (storing it in the cloud and accessing it only off a Chromebook or a computer running TAILS or Virtus booted off a thumbdrive. If you travel with a laptop, turn off the USB ports (to exclude that attack vector), use a screen privacy protector to protect against a (in this case literal) side-channel attack, and store your most secret data using steganography or in hidden encrypted TrueCrypt volumes (for plausible deniability); you and everyone you know should have end-to-

end PKI encryption (under either S/MIME (built in to Outlook and Thunderbird) or OpenPGP (PGP Desktop, netpgp, AGP, GPG4Browsers, Enigmail + GnuPG or Gpg4win, GPGTools (for Mac OS X), iSecureMail + iPGP or iPgMail (for iOS), Mailvelope for webmail)) for your e-mail (or an equivalent web-based solution such as SecureComs, StrongWebmail, or VaultletSoft; or leave drafts for your interlocutor in a webmail account to which you both have the password); you should avoid using mobile phones at all (even if you're running end-to-end voice encryption on all of them, e.g. Whisper's RedPhone for Android phones, or for J2ME phones PhoneCrypt or CryptoPhone) (and you should have InTheClear ready to wipe your phone when in danger of being taken). You should know something about sweeping for conventional surveillance (bugs) and self-defence, and you should be armed (and wear armor). Your organisation should have GPS-disabled end-to-end-encrypted satellite phones and should perhaps be experimenting with blackout-resistant technologies like mesh networks, e.g. NAF's Commotion (in case the national internet's shut). These are answers to real issues, but overkill for promoting freedom of access to information; don't be distracted by them until you've taken care of the more-important issues described in this paper.

The fields of online security, censorship, and circumvention, are fast-moving. Additional sources of advice from organisations investing ongoing effort in providing ICT support to activists working in dangerous situations include:

Internews' *Digital Security Toolkit*
Counterpart International's Information Security Coalition
Front Line Defenders' *Digital Security and Privacy for Human Rights Defenders*
Tactical Technology Collective (TTC)'s NGO-in-a-Box, Security Edition
EFF's *Surveillance Self-Defense* and *Defending Privacy at the US Border*
NDI's *Technology Tools for Activists*
Access Now's *Protecting your Security Online*
Онлайн безопасность для чайников
IT46's *Making the right choices: Recommendations for secure and sustainable hosting of independent media websites*
Global Voices' *Anonymous Blogging with WordPress & Tor*
Movements.org's *How to Organize on Facebook Securely*
Freerk Ohling's Internet Censorship Wiki
ONI's *Access Denied*
Freedom House (FH)'s Freedom on the Net
and (about mobiles) Safety on the Line
IWPR's CyberArabs (in Arabic)
FrontLineSMS's *User Guide to Data Integrity*
FIDH's *Les Bases de la Sécurité Informatique*
CPJ's *10 Tools of Online Oppressors*
Greenhost's *Basic Internet Security*
IT-Political Association of Denmark's Polippix
Jens Kubieziel's *Techniken der digitalen Bewegungsfreiheit*
International News Safety Institute (INSI)'s Safety Resources
InfoSec Without Borders IT help for NGOs
Small World News' Guide to Safely Using Satellite Phones
Privacy International's Human Rights Defenders' Privacy Workshop Curriculum
Australian DoD's Strategies to Mitigate Targeted Cyber Intrusions



TTC, FH, IFJ, the IMS, the DRC, Internews, Civil Rights Defenders, Videre, Digital Democracy, and others regularly hold courses throughout the world on cybersecurity for developing-country activists and journalists.

Postscript

Additional suggestions—from policy advocacy to activists' physical safety—are available from a wide variety of sources. Examples include ICNL's civil society survival tip-sheet, communications support from Advocacy International, the International Center for Policy Advocacy's Policy Advocacy Framework, hostile environment trainings from Centurion, technology support from Witness, journalist safety guides from INSI, and others.

This guide is dedicated to the many extraordinarily brave individuals who stand up to defend their own and others' rights in less-free countries—and to their family members who too often are also made to pay a price.

Postpostscript

"If you think it, don't say it. If you say it, don't write it. If you write it, [encrypt it; if you don't,] don't be surprised."