SpeakSafe

Media Workers' Toolkit for Safer Online and Mobile Practices

Internews
Local voices. Global change.

Acknowledgements

Digital and online tools are irreversibly changing the way professional and citizen media access, consume, produce, and share information. Whether researching stories using a shared computer in a newsroom along the Pakistan-Afghanistan border or talking to contacts in the refugee camps in Africa using mobile phones, journalists and media producers need to understand not just how to use these devices, but also how to protect themselves and the sources they rely on for information.

SpeakSafe is dedicated to journalists and media workers in the business of information. It is produced through Internews' Global Human Rights Program, which works to strengthen the capacity of media to report safely on human rights issues.

Editor and Producer: Manisha Aryal
Principal Researcher and Writer: Sam Tennyson
Copy Editor: Jenny Holm
Graphics and Icons: Ashley Low
Design and Layout: Citrine Sky Design
Production Coordinator: Ericha Hager

Internews thanks Kristen Batch for her advice on toolkit content and Josh Machleder, Svetlana Kimayeva and Djamilya Abdurahmanova for programmatic, moral and administrative support during the production process.

Toolkit reviewers include Internews' Innovation Advisors and Internews technical staff. We consulted with many Internews country programs and partner organizations around the world that share Internews' mission. Your work, expertise, learning, and input continue to inform our work and Internews thanks you all for your support.

While SpeakSafe was developed by Internews, it builds on educational and training materials produced by organizations working in mobile, internet and digital security and media and human rights issues. We have listed the links to these resources in the section titled Digital Security Links. This toolkit can be found online at www.speaksafe.internews.org.

Table of Contents

NOTES

Introduction

It's easier than ever to share who we are, where we are and who we know. Digital technologies have expanded the set of tools in media workers' toolkit and made the work of investigative journalists, citizen reporters, bloggers and other communicators easier. We now carry our address books on SIM cards, contact our sources using SMS, research our stories via search engines and Wikis, conduct interviews using audio and video chat, file our stories using email and make our and others' voices heard through websites, social networks and blogs.

However, we may be sharing more about ourselves than we realize or intend. Mobile phone conversations — and our location when the phones are with us — can be monitored; the emails we send and receive through popular services like Yahoo! or Hotmail can be read by people who work at our local Internet Service Provider (ISP) or at the Internet café we're using. And our activities on Facebook or other online accounts may be visible to others when we connect through unencrypted public WiFi access points.

While the Digital Age has introduced cool tools into our lives and increased our productivity, it has also exposed us and, by extension, our work and our sources to greater risks.

Until a couple of decades ago, information security for journalists meant taking steps to ensure no one was listening in on our phone conversations. Now, as we adopt digital tools to communicate better, the threats to privacy are keeping pace. In some countries, authorities require ISPs (Internet Service Providers) to block websites, to provide reporters' and bloggers' chat histories, and monitor posts on social networks and forums. Surveillance software is starting to pop up as email attachments to gain access to personal computers and office networks.

Those in power are not the only ones eavesdropping: organized crime gangs and freelance hackers are also tapping into journalists' computers through unsecured wireless networks and a host of other ways. In a recent high-profile example, former Gizmodo and Wired writer Mat Honan revealed that hackers had taken advantage of weak password recovery policies at Apple and Amazon to gain access to accounts that he had linked with his personal devices and several online services. As a result, they were able to remotely delete all the data on his smart phone, tablet and laptop, as well as any information he had backed up online. This was after they'd hijacked his Gmail and Twitter accounts. (You can read Mat's clear account of what happened at *Wired*.)

(By the way, we'll be using the term "hacker" quite a lot to refer to someone who intends to do harm to a website, a service or an individual, but we want to acknowledge the many "white hat" hackers out there – people who simply love to learn how things work, and who use their skills and knowledge to help others. For the time being, though, the word "hacker" is generally used in the mainstream press when referring to the "black hat" variety, and we've adopted that convention here for convenience.)

As people who dig for information, produce media content on critical social and political issues, disseminate facts, ideas and opinions through digital platforms, it is important that journalists and bloggers understand the sociopolitical contexts in which we operate. But we also need to understand the interests and technological capabilities of those (governments, organized crime groups, etc.) who want to limit the public's access to information and are taking decisive steps to curtail it. Finally, we need to make smart decisions and take action to protect ourselves (and the sources we rely on for our work) and ensure our own digital security.

This toolkit introduces reporters, journalists, bloggers and media workers to simple yet effective practices to maintain control of important information and communications. It also introduces several excellent online resources where you can find additional information, tutorials and software.

How we organize the information

This toolkit is intended to be useful whether you have a personal computer, share one (in a newsroom, cybercafé or press club) or do most of your work on a smart phone. We've chosen topics from a variety of online sources and divided solutions into three categories:

- **The Basics** – essential/urgent fixes, many of which we recommend you do immediately
- **Some Advanced Techniques** – a bit more technical, but useful to learn

- **More Resources** – related material, available for free on the Web, where you can get in-depth explanations and information about specific topics

Each topic also includes a checklist of recommended activities to get you started and help you chart/monitor your progress. They do not include every possible solution to specific challenges, but contain a variety of popular methods for tackling problems as they stand today.

Some assumptions

While this kit includes sections for dealing with computer viruses and compromised networks, the majority of recommendations assume that your device is not infected.

We acknowledge that Mac and Linux operating systems are increasing in popularity. However, the vast majority of PCs around the world still run on Windows and many producers and disseminators of content use these. This toolkit, therefore, focuses on Windows and Windows-based applications. We hope to provide similar information for Mac and Linux users in the future.

Not the last word on safety

There are developments in technology every day, as well as new threats. (Symantec, the maker of the popular Norton anti-virus program, estimates that more than 2,000 new viruses are released each week.)

This toolkit, published in October 2012, is intended as an introduction to information security and a guide to many related resources available for free on the Web. Please look for updates to this toolkit and to the websites highlighted in the More Resources sections.

Before you click...

This tool kit contains links directly to Web resources and applications that we hope will be useful for journalists and bloggers in their work. Be aware, however, that if you use an insecure connection to visit some of these sites, your activity may be visible to network administrators in your office, neighborhood or ISP (Internet Service Provider). Please read our **Safer surfing** and **Reaching blocked websites** section if you are concerned that visiting some of these websites may have negative consequences to you or your organization.

1: Keep control of your PC

Protecting your PC from viruses and other kinds of malware.

Connecting a PC to the Internet without protection is like leaving the door of your home open: Anyone can walk in. Studies have shown that unpatched and unprotected PCs can become infected in a matter of minutes when connected to the Internet and allow all sorts of other intrusions from strangers. Increasingly, smart phones are facing similar challenges.

While they've become a common problem for all of us, viruses and other kinds of malware ("bad" software intended to hijack your PC, spy on your activities or otherwise ruin your day) can have particularly serious consequences for journalists and bloggers.

At the least, a virus can interfere with your ability to work and post stories. You might lose access temporarily to your programs or files and, as a result, won't be able to get stories to your editor on time, research an article or make an online interview appointment.

Consequences can be more severe, though. Depending on the kind of virus, you can lose your work permanently, both your current project and everything that came before; or lose access to your email or chat accounts and the confidential communication in them. You can lose your contact list, something that you may have spent years building, potentially putting your most confidential and vulnerable contacts at risk.

Some malware can even allow a stranger to watch what you're doing online or learn your passwords for accounts you thought were private.

This section talks about some steps you can take to better protect your devices against viruses and other sorts of malware.

UPDATE YOUR ANTI-VIRUS APPLICATIONS

Most paid anti-virus applications will provide updates for one year before expiring. After that, the application will still work, but it won't be updated. If your license has expired, you'll want to purchase the latest version of the program, or alternatively, install a free anti-virus application.

The Basics

Get anti-virus software

Everyone can benefit from installing and regularly updating an anti-virus application, no matter what operating system (OS) they use. Anti-virus applications help deflect malware from our own PCs, but also help protect the PCs of friends and colleagues. (Just because a virus might not affect your particular operating system doesn't mean you won't be infecting a colleague's machine when you share an infected file.)

Use a combination of prevention tools to protect your PC:

- An *anti-virus* application that protects against infection from viruses and may be able to help remove a virus if you are infected
- An *anti-spyware* program to look for applications and cookies that send out information about you and your Web-surfing habits

- A *malware scanner* that can identify and remove *malware* — software that can harm your PC or capture your private information

Update everything

Viruses often take advantage of outdated software. Anti-virus applications, for instance, need to be updated regularly or they may not be able to defend your PC against new viruses. Keeping your operating system up-to-date is just as important. On your PC, make sure that the Windows Automatic Updates feature is enabled:

- Check the status of Windows Update: In Control Panel, click "System and Security" and then, under Windows Update, select "Turn automatic updating on or off"

By the same token, keeping your other applications up-to-date will help prevent security breaches.

You also can manually check for updates to your applications by visiting the developers' websites, or you can use an application like Secunia PSI to check for you. (**Secunia PSI** will also provide a link to the developer's site when available.)

- Download Secunia PSI

Turn on a firewall

When we connect to the Internet, whether it's through a cable, wireless connection or phone, we may not realize we're exposing our PC or mobile device to threats we can't see. For example, viruses called *worms* are designed to automatically seek out devices to infect. Once they successfully infect one machine, they immediately start looking for another on the same network to leap on. The SANS Internet Storm Center — a website devoted to tracking the potency of worms and other malware on the Web, currently estimates an unprotected Windows machine — one that isn't patched and doesn't have a firewall enabled — can be infected in an average of five minutes when connected to the Internet. (You can track the average "survival time" yourself at Survivor Time.)

A firewall can help prevent worms from burrowing into the devices you depend on for reporting, writing and other necessary tasks. It acts as a barrier against worms and other trespassers by blocking any internet traffic you didn't request or specifically permit. (Sometimes, firewalls are used by governments or Internet Service Providers to prevent users from accessing specific websites, but the sort we are talking about here prevent unwanted traffic from coming into your PC or mobile device.)

If you connect to the Internet through a *router*, you already have a hardware firewall working for you — a filter that blocks incoming traffic you didn't request.

But a software firewall on your PC or smart phone can provide extra protection against intrusions. Windows PCs come with a built-in firewall called Windows Firewall that is usually all you need to block most trespassers and alert you when applications try to connect to the Internet without your permission.

- Check that your firewall is enabled: In Control Panel, click "System and Security" and then, under Windows Firewall, select "Check firewall status"
- You can learn about a free alternative to Windows Firewall that includes some additional features, such as a dashboard that lets you monitor all your connections, at the Security in-a-Box website

Be proactive

The best protection against malware is our own behavior. Some good habits to adopt:

- Only download software directly from the application's official website, or from download sites that test for malware like FileHippo, Softpedia or Download.com
- Don't click on links in emails. Instead, copy and paste the link into your browser's address field
- Don't open an attachment in an email unless you know the person who sent it. If you are worried about an attachment that you have already downloaded and your anti-virus application doesn't automatically scan your email's Inbox, you can still check it by starting a manual scan of that file
- Don't install pirated software. It may be cheap, but it can come with extras you don't want, like malware! Consider free, genuine alternatives to the software you need. The website alternativeTo provides recommendations for free applications based on your operating system and what you're trying to accomplish. The website osalt offers a similar service, focusing on open-source programs.

STICK WITH ONE ANTI-VIRUS APPLICATION

If one anti-virus is good, two will be even better, right? Nope. Anti-virus applications usually require special access to your operating system and, when they see each other skulking around in the basement, can mistake one another as...viruses! They can also prevent one another from seeing all the files on your PC.

IF YOU DON'T HAVE MICROSOFT OFFICE...

Don't have Microsoft Word, Excel and other Office apps? There are several free alternatives. Some, like TextEdit and AbiWord, can fill in for single application, like Word. Others, like OpenOffice and LibreOffice provide a whole suite of programs.

If you share a PC:

If you share a PC at your news office, having an anti-virus application — one that you have configured to protect all users — is very important, since one person's behavior can affect the health of the PC for everyone.

If you do your news work or blog from a public IT cafe, you probably can't vouch for the safety of the PCs used there. If you are concerned about whether something you have downloaded has a virus, however, you may still be able to check it with a portable anti-virus application like Microsoft's Safety Scanner or with a free online scanner like TrendMicro's HouseCall or BitDefender.

- Scan your PC with HouseCall now
- Scan your PC with BitDefender now
- Visit the Microsoft Safety Scanner webpage

Some Advanced Techniques

There are other ways to protect your computer that are slightly more challenging, but provide practical benefits.

Disable Autorun in Windows

Has the PC you use at work ever been infected from a flash memory stick or a CD? Maybe you were copying a photo that had just come in fromthe field and — suddenly — alert messages start popping up. Some malware can hop from an infected device to a PC through the Autorun feature — a feature that automatically launches applications for our convenience, but can also allow malware to start working before you know it's there. Microsoft explains how to disable Autorun manually in all versions of Windows since Windows XP, and also offers online tools to switch the feature on or off:

- Turn Autorun off
- Turn Autorun on

INSTALL SOME NEW WINDOWS

If you're among the many people still using Windows XP–and some estimates suggest more than 40% of PCs connected to the Internet still do–it might be time to upgrade to Windows 7 or even 8. Microsoft has announced it will no longer support XP after April 8, 2014, and that means that XP users will no longer receive security updates after that date.

Close your ports

You can't see them, but your PC has ports that it opens to communicate with the outside world — 65,535 to be exact. Some of these are used for email, some for surfing the Web, some for online chats and so on. Just like an open window in your home, an open port can allow uninvited guests in, so you may want your PC to close any ports you're not currently using. You can check if your PC has any open ports with an online utility called Shields Up!. The website, which is largely devoted to making PCs more secure, is also a good source of information about online safety.

- Check if any of your ports are open and visible to hackers

Keep it legit

If you pay for anti-virus software, be sure it is a legal copy and that the application (and not just its list of viruses) is current. A pirated or "cracked" copy of any program is insecure.

Use a disposable version of your operating system

If you or (if you're lucky enough to have them) your IT support colleagues have spent countless hours re-installing your operating system and programs due to viruses or other software problems, you might want to consider using a virtual machine — a sort of temporary version of your software that you can throw away if it starts misbehaving.

A virtual machine — or "VM" for short — creates a protected environment, one that doesn't have access to everything on your PC and limits the damage that a virus or other malware can cause. If you open a suspicious file in this environment, for example, your virtual operating system (OS) might become infected, but it's unlikely to harm your "real" PC. Then you can toss out the infected OS and start with a new virtual machine (assuming you've kept a copy handy!).

Windows 7 supports this kind of virtual environment with a built-in feature called Virtual PC, though people who are unfamiliar with virtual machines might want to explore VirtualBox, a particularly user-friendly application that can run on Windows XP, as well.

- Windows 7 users can learn more about Virtual PC
- If you're new to virtual machines or don't use Windows 7, you might want to try VirtualBox
- If you'd like to learn more about Virtual Machines in general, you can find a lengthy article on the subject at Wikipedia.org

Make a "snapshot" of your hard drive or OS

When things go wrong, sometimes you just wish you could go back in time and have things the way they used to be. PCs allow us to do just this.

You can make a *snapshot* — a copy — of your PC's operating system while it's healthy and, if you catch a virus, restore things back to normal. Windows 7 includes this feature in Backup and Restore. To get started:

- Go to Control Panel and, under System and Security, click on "Backup your computer"
- Select "Create a system image" from the list of options on the left. You'll be able to save your current Windows files and settings, as well as your programs, to an external hard drive or a series of DVDs
- Microsoft explains in more detail how to save Windows 7 data and settings

If you want the option of making an exact copy of everything on a hard drive — sometimes called "cloning" the drive, several free backup programs can help. One of the most user-friendly of them is Easeus Todo Backup.

- You can download Easeus Todo Backup

When you're infected:

Common wisdom says there's only one way to truly keep your PC or mobile device safe from viruses and other malware: Don't use it.

Unfortunately, that's not very practical for journalists or bloggers who, after all, receive files and correspondence from their sources who may not be especially safety conscious. In case the worst happens, see our Basic Protection checklist for recommendations on dealing with an infected PC.

More Resources

Security in a Box from Tactical Technology Collective and Front Line Defenders

- "Protecting your computer from malware and hackers" — Security in-a-Box has step-by-step guides to:
  - Avast! Anti-virus
  - Spybot Search and Destroy
  - Comodo Firewall
- Digital Survival Guide: The Computer

Google's Stay Safe Online

- Phishing
- Malware

Basic Protection checklist

Prevent malware

On a PC:

- Download and install one application from each of the following categories:

  Anti-virus
  - AVG
  - Avast!
  - Avira

  Anti-Spyware
  - Super Anti-Spyware
  - Spybot Search & Destroy
  - Adaware

  Scanner/remover
  - Malwarebytes Anti-malware
  - Trend Micro HouseCall
  - Microsoft Safety Scanner
- Update the applications you installed
- Run a complete scan

If sharing a PC:

- Confirm that your User Account is protected by an anti-virus application and that it is up-to-date
- If you share a PC at your news office, discuss with your office administrator about adding anti-spyware and malware protection, if it isn't in place

MULTITASKING ANTI-VIRUS SOFTWARE UPDATES

If you work in a newsroom, you probably have several PCs around that could use a little updating. Download an update once and then installing it on all the PCs with the same operating system can save time and bandwidth. One application that helps you do this is wsusoffline.net.

NEVER TRUST AN OUTSIDER

You should always scan flash memory sticks, external drives, CDs and DVDs for malware.

- If you work from or blog at an IT café, you can bring your own protection (AVG Rescue Disk and Microsoft Safety Scanner run off a USB flash memory stick to check public PCs for malware) or you can run an online scan from services like TrendMicro's HouseCall or BitDefender

Update everything

- Update the operating system. In Windows, enable Automatic Updates
- Enable automatic updating for your anti-virus and other anti-malware applications
- Visit the home pages of the programs you have installed to confirm you have the latest version or consider using an application like Secunia PSI to check for you
- Set a repeating reminder to check for new updates

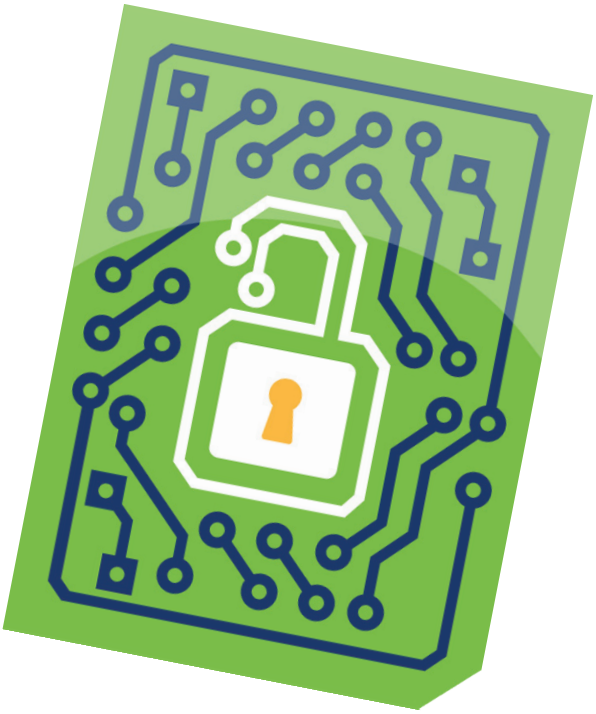
Turn on your firewall

- Confirm that your PC's firewall is turned on
- If you want extra protection, install an additional, free firewall like Comodo. You can find a step-by-step guide to using Comodo at the Security in-a-Box website, run by Front Line Defenders and Tactical Technology Collective

NOTES

2: Protecting your data

Protecting your PC or smartphone from viruses and other kinds of malware.



Your contact list, current research and archives of past articles and pictures are among any journalist's most precious possessions, but they are also attractive to competitors or anyone else who may want to find out who your confidential sources are or what you have researched for an upcoming project.

Losing these things can be disastrous. After all, what would you do if notes you'd accumulated from several interviews over the course of a month disappeared and you didn't have a backup? For many people, it means starting all over.

Here are some methods for protecting your work and resources:

The Basics

Start with a strong password

A lock is almost useless if it can be easily picked. Likewise, if your password is "password" or if it's the same as your username, it won't take much effort to unlock whatever you are protecting.

Tactical Technology Collective provides an excellent list of recommendations for making a strong password, including:

- Make it long
- Make it complex (see the list of top 25 passwords)
- Don't make it personal (a passphrase taken from your favorite book is less secure if everybody knows which book is your favorite!)
- Don't use the same password for more than one account

For fun, you can test various passwords in Microsoft's password checker to see how adding capital letters, numbers and special characters affects password strength. (As with any online password-checker, though, you should not use real passwords you intend to save!)

- See how length and other characteristics affect password strength on Microsoft's password checker
- Read more password tips from the Security in-a-Box website

Keep your passwords safe

You can protect your list of passwords with… a password. While it may sound silly at first, there are some real benefits. For one thing, you only need to remember a single password — the one that you use to lock and unlock your protected list of other passwords. And, unlike keeping your passwords in, say, a text file or a piece of paper on your desk, a "password safe" can protect your passwords with encryption in case it's lost or stolen.

There are several password safes that do the job. KeePass, which is free, can be carried on a flash memory stick and has some extra features such as letting you lock up your password list with both a master password and a keyfile (a file that must be present on the PC for your password to be accepted).

- Download KeePass
- You can find a tutorial for using KeePass on the Front Line Defenders and Tactical Technology Collective's Security in-a-Box website

IS THIS YOUR PASSWORD?

List of the top 25 most commonly used passwords:

1. password
2. 123456
3. 12345678
4. qwerty
5. abc123
6. monkey
7. 1234567
8. letmein
9. trustno1
10. dragon
11. baseball
12. 111111
13. iloveyou
14. master
15. sunshine
16. ashley
17. bailey
18. passw0rd
19. shadow
20. 123123
21. 654321
22. superman
23. qazwsx
24. michael
25. football

Lock up your data

A User Account password — the password you may be asked to type on the Windows welcome screen, can be a convenient way to protect your settings from being changed without your permission, but it doesn't protect your files from someone with physical access to your computer. For that, you'll want whole-drive encryption to scramble the contents of your files.

Bitlocker, an application in Enterprise and Ultimate versions of Windows Vista and Windows 7, can lock up both the PC you use for your news work as well as external hard drives – like those you might use for backing up your data.

- If you already have a compatible version of Windows, you can turn on Bitlocker in Control Panel by clicking "System and Security" and then "Bitlocker Drive Encryption"

If you don't have the compatible version of Windows, you and your colleagues can still get whole-drive protection with the free application called **TrueCrypt.** TrueCrypt isn't as streamlined as Bitlocker, but comes with additional options: It can run off a portable flash memory stick so you can take it with you; it's flexible and can be used to encrypt your hard drive or a single folder; and it gives you the option of locking up your files with a password, a keyfile or both.

- Download TrueCrypt
- The developers provide a tutorial for using TrueCrypt

DELETING UNWANTED COPIES OF FILES

When you unlock — or decrypt — a file on your PC, it can remain available on the PC later. You can use a utility like CCleaner to delete these unprotected (and unwanted) copies.

If you share a PC:

Network administrators in your newsroom or public IT cafe may have the ability to copy the contents of any flash memory stick or other device that you bring without informing you, depending on the access they have to PCs on the network. Consider using TrueCrypt to protect files on your device, but also be aware that, once decrypted, those files are potentially visible to the people who run the network, too. Get to know their policies and their practices.

Also, if you share a PC, make sure that folders on the PC aren't being shared with other, non-administrator computers on the network: right-click a folder and select the Sharing tab to see whether the contents of that folder are being made available to other PCs (for instance, laptops used by other reporters or bloggers) on the same network.

- Learn about file sharing at Microsoft's support site for Windows

Keep everything backed up

Viruses, power outages, hardware failures and theft… all pose threats to your data, so it's important to keep protected copies of your work, your contacts and anything else that is essential to your work as a journalist.

There are plenty of methods for backing up files (the best one being the one you actually follow!). Whatever method you choose, stick to these guidelines:

- Keep two backups of your data: one close by, on an external device or media (CD, DVD) and…
- one at another location, such as a friend's house or in "the cloud" (using an online file-sharing or backup service). Be careful not to rely only on cloud-based storage, though: if you lose access to your online account, you lose access to your backups, as well.
- Back up on a regular schedule — automate it if you can. Weekly is good
- Protect your backup with encryption and a strong password

BACK UP YOUR BACKUP

Many online services such as Dropbox and Mozy provide limited storage for free, but you should make sure that you keep an offline copy, too, and protect any files you back up to the Web or external drive with encryption.

Keep these principles in mind, even if you are lucky enough to have an automatic back-up system in your newsroom. A power surge, fire, flood or seizure by authorities can quickly put your backups out of reach.

Some popular ways to back up your PC:

1. You can drag-and-drop files to an external drive, taking care that the drive or folders on the drive are encrypted and protected with a password. If you are unsure how to encrypt your external drive or folders you'd like to place there, see our Lock up your data section above or visit the Security in-a-Box website for an introduction to TrueCrypt
2. Windows 7 users can use Backup and Restore to save files from the most common locations (e.g. My Documents) to an external drive, to DVDs or to a network drive, again taking care that the destination is password-protected.
3. People who use other versions of Windows or want more control over their backups can download a free application like the frequently-recommended **Cobian Backup** that includes an encryption feature and an automatic scheduler so you don't need to remind yourself when to refresh your copies.
    - To get started with your first Backup in Windows 7, open Control Panel, click System and Security, and then Back-up and Restore
    - Download **Cobian Backup**
    - Visit the online tutorial from Front Line Defenders and Tactical Technology Collective

TAKE THE INITIATIVE TO PROTECT YOUR DATA

Windows System Restore can help retrieve operating system files and your User Account password can protect your settings, but neither is intended to significantly protect your data.

Remove details from Office documents

Microsoft Office documents, such as Word and Excel files, contain information about who created the document, who last read it or edited it and other details. If you don't want to include this kind of information in your documents – perhaps you wish to protect a source who has shared a report with you, not realizing they were leaving a virtual trail, you can tell Office 2010 and more recent versions to remove much of this identifying information.

- With a document open, choose File in the main menu, then Info. Look for the section called Prepare for Sharing, and choose the Check for Issues icon. The Inspect Document feature will look for personal information, comments and even invisible content, and then give you the opportunity to delete it.

Some Advanced Techniques

Disable Remote Assistance and Remote Desktop

Windows lets you receive technical assistance online from people in remote locations when disaster strikes. But these useful features can be abused. To avoid unintentionally sharing access to your PC, you can make sure these features are disabled by default (you can always re-enable them later, if needed):

- In Control Panel, select System and Security and, under System Settings, click on "Allow remote access" to see your current status. Un-check the box for "Allow remote assistance connections to this computer" and then choose the radio button that says "Don't allow connections to this computer"

Store files in a "hidden volume"

TrueCrypt gives you the option of protecting some of your data in a hidden compartment inside one of your encrypted folders so that, if you are forced to reveal your password, files in the hidden compartment won't be visible. Setting up a hidden volume can be tricky, though, and not understanding how they work can result in accidental deletion of the data you keep in there. Check out both the explanation and tutorial below before you risk your photos, audio interviews or other material that you consider crucial for your work.

- Read this explanation of hidden volumes at the TrueCrypt website
- Get a step-by-step tutorial at the Security in-a-Box website

Make a disk "snapshot" of your hard drive

If you want to back up absolutely everything, right down to your operating system's settings, you can make an exact copy of your entire hard drive. Some backup programs bundle this feature into their applications, and one of the best for ease-of-use and features is Easeus Todo Backup.

- Download Easeus Todo Backup

More Resources

Passwords:

- How to create and maintain secure passwords (Security in-a-Box)
- Step-by-step guide to using KeePass — Secure Password Storage (Security in-a-Box)

Encryption:

- How to protect sensitive files on your computer (Security in-a-Box)
- Using TrueCrypt (Security in-a-Box)

Backing up:

- How to use Cobian Backup on a PC (Security in-a-Box)

Data Protection checklist

Create good passwords

On a PC:

- Read Front Line Defenders and Tactical Technology Collective's recommendations for strong passwords
- Download KeePass and create a new database, locking it with a strong password
- Transfer your passwords into KeePass. From time to time, update your passwords to improve their strength
- Make sure you include your password database in your backup plan

Encrypt your sensitive data

On a PC:

- To encrypt your hard drive, check if your version of Windows already has that capability with Bitlocker. If not, download TrueCrypt and read the tutorial at the website
- To create encrypted folders (not the whole hard drive) or hidden folders, download TrueCrypt
- Before you start encrypting a hard drive, make a copy of all your data on an external device

KEEP IT SECRET, KEEP IT SAFE

Pssst! A password isn't so secret if you share it with others. Also, use different passwords on different accounts or services on the Internet.

- Find a tutorial for your method of encryption:
  1. Windows Bitlocker
  2. TrueCrypt

If sharing a PC:

- Assuming that you may not have permission to install software on the PC you share, you can carry an encryption program with you: Download TrueCrypt, open the installation file and select "Extract" instead of "Install" in order to put the program onto a flash memory stick
- Read the tutorial for using TrueCrypt

Back up your data

Encrypting the data on your PC or smartphone helps prevent others from accessing it.

On a PC:

- Decide what you want to back up. Will it be everything including your operating system and programs? Or do you want to back up just your data – your files, email, images…?
- Get an external hard drive with sufficient capacity for the data you will back up
- Pick a method for backing up (for instance, using a third-party application like Cobian Backup)
- If the method you chose for your primary backup does not provide encryption, encrypt your external device with Bitlocker or TrueCrypt. If the drive is lost or stolen, your data will remain locked
- Decide how you will make your second backup. Another external device or an online service?
- If you back up manually, without a specialized application, set reminders to back up regularly and make it a routine

DON'T KEEP BACKUPS ON YOUR PC

Don't back up your files to another partition on your PC. If the PC is stolen or if the hardware is damaged, you'll lose both the original data and your copy.

3: Safer email

Using HTTPS and a safer email service to keep your communications private.

Sending an email is a bit like sending a letter through the postal service in an unsealed envelope: as the letter gets handed around the postal system, it can be read by anyone who holds it. Online, your Internet Service Provider (ISP) and other important players in the network are "holding" the email that you write and they might decide to read it.

So what? Most of what you send and receive won't be of interest to anyone but you and the person you are writing. Still, work-related emails may contain information that you'd rather not share with the ISP or the authorities that control it. Perhaps you are sending your latest article to your editor or conducting an email interview with a human rights activist whose comments, while useful as background to your story, would get him or her into trouble.

Whatever the case, there are plenty of reasons not to make your emails available to someone other than the person you are writing to. Here are some simple steps you can take to make your email more secure:

HTTPS IS A TWO WAY AFFAIR

An HTTPS connection protects email on its journey to the email provider, but the person receiving your email must use HTTPS to provide the same protection when they read it.

The Basics

Use HTTPS

If you use a free public webmail service like Gmail or Hotmail, make sure it supports HTTPS connections between your PC and its servers. Both Gmail and Hotmail support this feature, though Hotmail makes it an option that users can enable it manually in their Settings. (If your news organization or publication has its own email service, as the administrator how they are securing connections to the email server.)

If you get your email through a browser, one easy way to make sure you use HTTPS for your session is to bookmark the full URL (e.g. https://www.somemailservice.com). Your webmail service must also support HTTPS but, if it does, you won't accidentally be bumped out of an HTTPS connection after signing in.

HTTPS connections create an encrypted tunnel between you and a website's server (that's the computer on the other end that "hosts" the site). When you communicate with a website through HTTPS, it's as if you are talking to a friend through a cardboard tube so that others in the area can't hear what you're saying.

You can see if your email service uses secure connections right now: Sign into your account and, in your Inbox, look at the URL in the address field at the top of your browser. If it starts with "HTTPS" (with an "S" on the end), you're using SSL. If not… sign up for a free account with a service that offers secure connections.

BOOKMARKS: SIMPLE BUT POWERFUL DEFENSE

If you get your email through a browser, one easy way to make sure you use HTTPS for your session is to bookmark the full URL (e.g. https://www.somemailservice.com). Your webmail service must support HTTPS, but, if it does, you won't accidentally be bumped out of an HTTPS connection after signing in.

PASSWORDS CAN BE YOUR WEAKEST LINK

A weak password may be the easiest way for someone to gain access to your email account, as several politicians have painfully learned in recent years. Remember: Make it long, complex and not guessable!

Again, if you are using Gmail, you should already be connected via HTTPS automatically. If you use a Hotmail or Live.com account, you can add HTTPS protection by following these instructions from Microsoft's "Serious About Safety" site:

1. In Hotmail, click **Options**, and then click **More options**. Under **Managing your account**, click **Account details**. You might be asked to provide your password.
2. Under **Other options**, click **Connect with HTTPS**. Click **Use HTTPS automatically**, and then click Save.

Use an email client

You can configure an email application like Outlook or Thunderbird to connect through SSL automatically. Email applications also provide some protection against losing your email forever if your account is hijacked, as they store a copy directly on your PC or flash memory stick. Thunderbird usually configures new email accounts for SSL if a secure connection is available, but you can also confirm your settings manually.

- Find out how to configure your email account in Thunderbird to connect by SSL

You're sending more than just your message

When you send email to a source, your editor or anyone else, you also are sending additional information that you may not see, but which can reveal more about you, or your message, than you'd intended. For instance, even an email with encrypted contents can expose what you've written in the Subject line (see more on this in **Some Advanced Techniques** below). Also, every email sent contains information in something called a *header* that can reveal the trail that an email took on its way through cyber space to the recipient, or the original email address that sent the email. In some cases, that can be useful — for instance, if you want to know if a friend actually sent you an email that appears suspicious. But it can also be revealing about our own emails if they are intercepted. Here's how to view the header in Gmail:

1. Log into your account and go to your Inbox
2. Select an email and open it
3. In the View dropdown menu, select "Show Original"
4. You'll now see the header

With this in mind, you may wish to try Tor or a VPN (see the Safer Surfing section for more on Tor and VPN) to obscure your location and IP address (the address associated with your particular PC or access point).

Think before opening, replying or clicking links

Maybe you've received a note that appeared to come from a professional acquaintance or fellow blogger that and announced he or she had been mugged while visiting a foreign country and asked you to send money right away. Or perhaps you got an email that said it was from your email provider, with the alarming news that your account will be closed unless you confirm your password. This sort of attack, which uses authentic-looking emails to trick you into some action (like giving up your password or sending money), is called *phishing* and it's so common now that it has become part of the background noise of our Inboxes.

The dangers, though, are quite real, and in some cases phishing emails are written very carefully to target specific people and organizations — so-called *spear phishing*. In May 2011, Google announced it had spotted a massive campaign in which emails were sent to hundreds of people in governments and NGOs, appearing to come from friends or colleagues of the recipients. In reality, the emails came from hackers who had included links back to servers in other countries in order to access who-knows-what. As journalists, we have to consider that we may be special targets for this sort of attack. Exercising some caution when navigating our Inboxes may help:

Don't click on links in email. Innocent-looking links can send you to a different address from the one displayed, or can wind up injecting a virus onto your PC. If you have been sent a link and it

appears to be authentic at first glance, copy the address and paste it into your browser.

Don't open attachments in email. Attachments such as images and documents may contain viruses that install when double-clicked. If you know the sender and you expected to receive the attachment, make sure that your anti-virus application scans attachments before you open them. Never open attachments from someone you don't know.

Disable images. Images in email can contain hidden links to websites or computers elsewhere. Merely opening the email can lead to other consequences, such as unintentionally downloading some code to your computer. Disabling images in your email will reduce the chances that someone can use this method of attack.

1. Learn how to disable images in Gmail
2. Learn how to block images in Outlook
    - Learn how to turn on 2-Step Verification for your Google account

Create an anonymous account for work

You may wish to keep a separate email account – one that is not associated with your real name, address, mobile phone number or other identifying information, that can aid your privacy when you work on a sensitive project and limit the damage to your personal email and contact list if the account is compromised (and vice versa).

Make sure you're not forwarding your email

Many email accounts, including Gmail, now let you automatically forward copies of your correspondence to other email addresses. That can be very useful for journalists who may need to keep more than one account active. If someone gets access to your email account, however, they can add their own email address to your forward list and receive copies of your emails without ever logging into your account again. Check in your Account Settings to make sure no one has added their Inbox to yours.

- Learn how to check your forwarding settings

Review your account activity

Some webmail services, such as Gmail, let you review your account activity so you can see exactly when and where the account has been accessed.

- Learn how to access your last account activity in Gmail

Don't link accounts

Some Web services now let you use the credentials of a partner service to sign in — for instance, using the credentials of an email account to also "unlock" a social network account so you can track updates to one service while using the other. That can be a great convenience especially if you need to publish stories and then promote them across social networks, but it also means that someone who learns your password for one account may suddenly instantly have access to the other, as well.

Use strong authentication

Some Web services let you to protect your account with a combination of information; for instance, a password *and* a code sent to your mobile phone. That way, a person trying to access your account needs both sets of information. Happily, this sort of extra protection is catching on — Facebook, Dropbox and other popular services now offer this feature as an option. You can enable protection for your Gmail account, for instance, in Google Account Settings.

If you share a PC:

If you share a PC in the newsroom or public IT café, private communication presents a special challenge. In addition to the risks that you can see in your physical environment, there may be risks you can't see, like keyloggers — a type of malware that can record your key strokes, or other malware.

Bring a portable browser with you, one with security add-ons installed (see Safer Surfing section for more information on these add-ons) or one that comes as part of an anonymity package like the Tor Browser Bundle. A portable malware scanner, like Microsoft's Safety Scanner or Comodo Cleaning Essentials can run from a flash memory sticks and detect common threats as well. But be aware that other exploits and even legitimate network management software may compromise your communication and not be recognized as malware.

4: Safer surfing

Adding security features to your browser and a more private connection to websites.

The Web is a powerful tool for journalists and the people they reach, but, like any tool, it is important to learn how to use it to avoid accidents.

Some webs can infect your browser or PC without you clicking on any links in the page. Visiting a website for research or for email through an insecure connection — one in which your activities can be monitored closely — might let someone collect data about your habits and location. As we mentioned in Safer Email, connecting to a website through HTTPS is safer than through a regular HTTP connection.

These steps will help add an extra layer of security on your browser.

(If you need to surf anonymously, be sure to see the Some Advanced Techniques and More Resources sections.)

The Basics

Use a safer browser

Companies may debate which Web browser is the most secure, but Firefox currently has the most Add-Ons with security and privacy benefits.

PROTECTING YOUR SEARCH RESULTS

Some search engines can protect your search results with a secure HTTPS connection. Google and DuckDuckGo.com are two that support the feature. DuckDuckGo has a policy not to track its users' search history.

Add-Ons are small applications that add new features to a browser. Some of the most useful for Firefox include:

- NoScript: Prevents Web pages from installing applications or launching a program on your PC without your knowledge
- HTTPS Everywhere: Automatically shows users the HTTPS versions of websites – versions in which the connection between your PC or phone and the website are encrypted. The list of sites for which this Add-On works is small, but includes many popular ones
- HTTPS Finder: Lets users add additional sites to the HTTPS Everywhere list of protected sites
- BetterPrivacy: Deletes long-term "cookies" in your browser that may be used to track you
- WOT (Web of Trust): Provides ratings for a website's privacy and trustworthiness, based on the votes of other Web users
- Perspectives: Checks the authenticity of the SSL certificate used by secure websites to spot potential fakes

You can find more Privacy & Security Add-Ons on the Mozilla website.

Use Chrome? You can also find some security extensions for Google's browser, including HTTPS Everywhere, Perspectives and WOT.

Check your security settings

Browsers remember a lot about you and your habits unless you tell them not to. As a journalist, that information may be special interest, especially if your work affects large companies or individuals

in power. To avoid typical surveillance issues, you can limit what Firefox remembers and add some other protections in your Options panel. To get started, select Tools from Firefox's drop-down menu and then Options:

On the Security tab:

- Select the checkbox *Warn me when a website tries to install an add-on, as well as the checkboxes to block attack sites and block web forgeries*
- De-select the checkbox offering to *remember passwords for sites*

On the Privacy tab:

- Select the checkboxes marked Tell web sites I do not want to be tracked, and Always use private browsing mode

Use a VPN

A VPN — or Virtual Private Network — can provide a tunnel between your PC and a server in another country, giving you greater privacy when you surf the Web, research articles or conduct interviews online. (It doesn't prevent the content you send and receive from websites from being visible to the company that runs the VPN, however. For that, you still need to connect to a website that supports HTTPS! It also does not prevent a VPN administrator from maintaining a list of its users and all of the sites that they visit.)

A few VPNs provide services for free, including:

- Psiphon 3, a stand-alone VPN client that can run from a USB flash memory stick or on your PC, automatically updates itself with new IP addresses of servers in the Psiphon service
- RiseUp VPN is available to anyone with a free RiseUp.net email account and can be accessed through a VPN application, like OpenVPN. OpenVPN is also available as a portable application
- Hotspot Shield, which is ad-supported, can be installed onto a PC, directly

It's important to remember that a **VPN does not provide anonymity.** When you establish a connection with a VPN service, the administrators there know as much about you as your ISP would, including what websites you're visiting.

- Learn about Psiphon 3, a free VPN solution, by sending a blank email to **get@psiphon3.com**
- Get instructions for configuring RiseUp VPN service from RiseUp.net
- Download HotSpot Shield

Use Wi-Fi hotspots with a protected connection

If you use Wi-Fi to connect to the Web, whether at a public access point or in the newsroom, make sure that your wireless connection to the router is protected with WPA or WPA2 encryption (WPA2 is best), and avoid places that use WEP encryption or that don't provide any encryption at all.

In many public access points, when you open a browser, the first thing you see is a Web page asking for a password. That may look reassuring, but it only means that access point's owner wants to control who has access to their Internet connection. Unfortunately, your connection to the router is not protected.

You can tell if your connection to a Wi-Fi access point is protected by right-clicking the network icon in the lower-right corner of your screen and hovering your cursor over the name of the network – the text that pops up will tell you if the connection is protected and in what format. You can also use a free utility like InSSIDer to get more detailed information about connections available in your area. **Even when using a protected hotspot, though, you should still connect to your favorite websites through HTTPS, or use a VPN.** Keep in mind that a VPN protects your connection locally but does not prevent someone running the VPN from seeing your activity on a website that is not HTTPS.

ARE COOKIES GOOD OR BAD?

Are cookies good or bad? The tags that websites insert into your browser to help them remember you or to track you across the Web are neither, really.

Some cookies are useful – for instance, cookies that allow you jump from one section of a subscription website to another without having to retype your password on every page (have you ever signed into Gmail and then opened a Google Calendar from the same account without having to sign in separately?). Other cookies, however, may be used to track the websites you visit and share that information with someone who wants to use it against you or to harm you.

Some browsers let you choose whether or not websites can place a cookie in your browser. Google Chrome, for example, lets you "Block third-party cookies from being set" in its content settings, which prevents the installation of some cookies that may be in advertisements from being installed. To enable this feature, type "chrome://settings/content" into Chrome's address bar.

Recently, some browsers have started to include an additional "Do not track" option in their privacy settings (Firefox does this in a checkbox at the top of its Privacy Settings).

HOW PRIVATE IS PRIVATE BROWSING MODE?

Is Private Browsing mode private? Most browsers allow you to prevent the browser from remembering your browsing, downloading or searching histories. It does not keep you private on the Web, however: Your ISP and the administrators of the site you are visiting know where you are and what you're doing, unless you take steps to protect your connection and use an anonymizing tool.

- InSSIDer is a free utility that displays information about Wi-Fi hotspots in your area.

If you share a PC:

- If you share a PC at your newsroom or IT café, it may be difficult to browse privately. In addition to the challenges of the physical environment, you may be compromised by malware or, in the case of some businesses, by software that tracks employee behavior.
- While you can't guarantee privacy, there are some steps you can take to improve your protection. For instance, you can run a portable malware scanner like Microsoft's Safety Scanner or Comodo's Cleaning Essentials, from a flash memory stick to check for malware before you surf. Keep in mind, though, that legitimate PC management software that tracks your activities might not be recognized as malware.
- A portable VPN and portable browser that has security add-ons installed may help. Likewise, running the Tor Browser Bundle, which is also portable, can provide some local privacy, as well as anonymity on websites you visit.

If you use a smart phone:

- Mobile phones run special versions of browsers made for their platform and these may not include Firefox or support the Add-Ons listed above.
- If you use an Android phone, you may already be able to take advantage of some anonymity features offered by The Guardian Project's Orbot.

OPENING DOWNLOADED DOCUMENTS

The Tor team advises users not to open downloaded documents while still online, as this can unintentionally cause your PC to broadcast information about the PC and you.

THE DIFFERENCE BETWEEN VPN AND TOR

What's the difference between a VPN and Tor? A Virtual Private Network encrypts your connection between your PC and one VPN server, perhaps one in another country, so that users in your immediate area - like your ISP or people who share an unprotected Wi-Fi access point with you, can't capture your personal information. However, people who work at the VPN have the opportunity to see where you are connecting from, what your connection's IP address is, what websites you are visiting and – if you use unprotected email – what you are writing and reading.

By contrast, connecting through Tor (The Onion Router) is a little like having three VPNs strung together, with each one only aware of the "hop" immediately in front of it or behind it in the chain. That way, the first server knows that you are connecting to the Web – but not the address of the site you are visiting, and the last server knows that someone is visiting a particular website – but not who.

See Mobile Active's instructions for browsing the Web anonymously with Orbot.

Some Advanced Techniques

Use Tor to anonymize your location

Tor (The Onion Router) cloaks your Internet connection in three layers of encryption and then peels them off, one by one, before sending you to the website you wish to visit. By providing additional "hops" in the middle of your Web journey, Tor masks the websites you visit from your local ISP, while also hiding your physical location from the websites you visit.

As a secondary benefit, you may find that websites that are normally blocked where you live are available when using Tor Browser Bundle, which includes a portable browser pre-configured to properly work with Tor.

If you want Tor's protection for other Internet services like Instant Messaging or email, read the developers' website carefully before proceeding: As they stress, you won't enjoy any of Tor's benefits unless you properly configure your application to run with it. Also, the Tor developers recommend not installing additional add-ons on their portable browser. (The browser does come with HTTPS Everywhere and NoScript add-ons pre-installed, however.)

Use OpenDNS or Google Public DNS

The Domain Name System, or DNS, is the index of the Internet. It takes domain names you type — like "yahoo.com" —

TOR CAN BE SLOW

Because Tor runs through several servers in a chain, it may slow down your Web surfing. You can always reserve your use of Tor for sensitive work and use a regular connection for more mundane tasks.

and translates them into very specific, numbered addresses like "72.30.38.140"so your browser finds the exact server in the exact location that you need for the exact website you want.

The Web depends on DNS to work properly, and users put a lot of trust in it.

Unfortunately, a DNS server might be hijacked or its directory re-written in order to block websites or send users to fake versions of the webpages they were expecting.

Both OpenDNS and Google Public DNS are free services that have done a very good job protecting their servers. They also don't block websites (though OpenDNS provides optional content filtering for parents).

- Find instructions for changing to OpenDNS
- Find instructions for changing to Google Public DNS

ANOTHER REASON FOR HTTPS

When your PC tries to establish an HTTPS connection with a site, your browser will check the site's SSL certificate first – a sort of ID card that's needed to complete the connection. If the certificate looks invalid, you'll get a warning in your browser, something that a regular HTTP connection to the same site would not be able to provide.

More Resources

Front Line Defenders and Tactical Technology

- VIDEO: ONO Robot's Guide to Safe Surfing
- How to Remain Anonymous and Bypass Internet Censorship

How to Bypass Internet Censorship

- How to Bypass Internet Censorship

Freedom House

- A Review of Censorship Circumvention Tools

Reporters Without Borders

- Handbook for Bloggers and Cyber-Dissidents
- 2012 report on "Enemies of the Internet"

Google Online Safety tips

- Safe Networks

Electronic Frontier Foundation

- How to Blog Safely (About Work or Anything Else)
- Install the HTTPS Everywhere Add-On for Firefox or Chrome

The Internet Censorship Wiki

- Filtering and Ways to Bypass it

Mozzila.org (Add-ons)

- NoScript
- WOT
- Perspectives
- HTTPS Finder

Global Voices

- Anonymous Blogging with WordPress & Tor

Mobile Active

- Mobile Anonymity and Censorship Circumvention: How to Browse the Web Anonymously on Your Phone
- A User Guide to Orbot: Anonymized Tor Browsing on Your Mobile Phone

Safer Surfing checklist

On a PC:

- Use Firefox
- Install privacy and security Add-Ons
- Change the browser's settings to avoid recording information you don't need or want
- Increase your local privacy by using a free VPN, or use the Tor Browser Bundle for greater anonymity
- Avoid being redirected to fake websites by using OpenDNS or Google Public DNS

If sharing a PC:

- Check the shared PC for malware
- Use a portable VPN and browser, or use the Tor Browser Bundle

On a smart phone:

- See what browsers are compatible with your phone and what Add-Ons — if any — are available
- If you use an Android phone, you may already be able to take advantage of some privacy features offered by The Guardian Project

5: Safer Wi-Fi

Keeping the wireless connection to your router safe from eavesdroppers and other "bad guys."

Public wireless access points make it possible for journalists to do their work from just about anywhere — coffee shops, hotels, schools or airports. But they're rarely protected with encryption and that makes them popular targets for hackers and other people who want to monitor unprotected *traffic* — the bits flowing up to and down from the Internet. That might include your email, Facebook posts or Tweets.

Developer Eric Butler brought this to everyone's attention in late 2010 when he released a free add-on for Firefox called Firesheep, which makes it easy for just about anyone with a laptop to take over your Facebook or Twitter session while you're signed in, read your personal messages and post an update pretending to be you. The add-on has had more than 2 million downloads since being introduced.

(Luckily, this particular threat can be defeated by connecting to web-sites through HTTPS. See the Safer Surfing section for more on that topic and other ways to protect your connection in public places.)

Hopefully, if you have a Wi-Fi access point at your newsroom, it's already protected with WPA or WPA2 encryption to keep strangers out. But if your router hasn't been "hardened" to prevent attacks yet, take a few minutes to adjust its default settings.

IT'S NOT ALL IN A NAME

Some people give their router a frightening name to deter uninvited users (e.g. "GetYourFreeVirusHere"), but you don't want to count on it for protection.

The Basics

Change the administrator password

Most routers have a default password enabled when you receive them — a password that you need to type before you can change even the most basic settings. That's a good thing. However, most of the default passwords that get used aren't very hard to guess. (If you're curious you can compare the default passwords for different routers.)

To avoid making it easy for someone with direct access to the router to change your settings, you'll want to upgrade the password to a strong one. Your router should have come with a user manual that explains how to access its settings directly through your browser, usually over an Ethernet cable, or you can download an electronic copy of your router's manual from the manufacturer's website for guidance.

Before you dive in, it's a good idea to write down your router's default IP address (usually 192.168.1.1 or 192.168.11.1) and the default administrator's username and password in case you need to reset the router and start again later.

Once you've connected your PC to the router and signed into the dashboard – the area that lets you control how your router behaves -- you're likely to see a lot of links, buttons and tabs to choose from. Your router's manual would be handy just about now, but if you can't find it, you're likely to find controls to reset the router's password in any area marked for Administration.

- Get more tips about creating strong passwords from the Security in-a-Box website

Turn on encryption

You should only use access points that provide encryption between your PC and the router to help protect your data from eavesdroppers in your immediate area.

To make sure you have encryption enabled, first follow the steps mentioned above to sign into your router's settings, and then look for the wireless security settings. The location of these settings will depend on the manufacturer of your particular unit. With security settings open, choose WPA or WPA2 from the list of available types of encryption (WPA2 is stronger, though not all older routers support it) and create a strong password – one that is long, complex and hard to guess.

- Get more tips about creating strong passwords from the Security in-a-Box website

Disable WPS (Wi-Fi Protected Setup)

It's rare that tech manufacturers make security easier for ordinary users, so the introduction of WPS, a system that lets you share a password with a PC just by pressing a button on the outside of the router, was a welcome change. In late 2011, though, developers revealed that, even if you don't use the feature, having it enabled on your router can cause your network to "cough up" your encryption password to someone probing the network.

Tactical Network Solutions (TNS) has made a free hacking tool called Reaver to demonstrate the vulnerability and says Reaver will reveal a WPA/WPA2 password, "in 4-10 hours, depending on the (router). In practice, it will generally take half this time to guess the correct WPS pin and recover the passphrase."

To keep your encryption key protected from intruders, disable this feature in your router's dashboard.

Turn off WAN, WLAN or remote administration

Out of the box, most routers are configured to allow someone to connect to them remotely, such as a technical support expert at your ISP who may want to help you get set up. Unfortunately, your router can't judge if someone trying to connect has good or bad intentions, so it's best to simply disable this feature.

Some routers now let you turn off something called WLAN (or Wireless LAN) administration, too. If you turn off WLAN administration, it means the router won't allow anyone to access its settings unless they are connected to it directly by an Ethernet cable.

HIDDEN ROUTERS AREN'T REALLY HIDDEN

You can hide your router from your neighbors by telling it not to broadcast its SSID (its name), but your router isn't invisible to anyone running InSSIDer or other free WiFi utility, so don't count on this for security.

Disable UPnP

Universal Plug and Play, or UPnP, is a convenience feature in most routers that lets other devices on your network control some of the settings without requiring you go through the drudgery of making adjustments manually. Video game consoles, printers and other devices sometimes use UPnP to tell the router to accept incoming connections from the Internet that normally would be refused – a potential door into your network that you probably don't want. Simply disable it and you won't miss it.

Some Advanced Techniques

MAC address filtering

If restricting access to your network by a password alone isn't enough for you, you can also tell your router which devices have permission to use it. In the process, you'll block any devices that don't have explicit permission, even if they have your router's encryption key.

How is this magic accomplished? Every PC and mobile device has a Media Access Control (MAC) address, a sort of identity card that it carries around to help distinguish it from other devices. In your router's dashboard, you'll find a section devoted to MAC filtering that lets you save a list of these addresses so your router knows which ones have permission to join the network. Any device not on the list is blocked by default.

A word of caution: While this sort of filtering can help you control access to your network when used in combination with other safety practices, it's important to remember that **MAC address filtering does NOT replace password protection, encryption or other safety measures for your network.** Filtering, by itself, offers no encryption protection between your PC or mobile device and the router, and, while not a trivial task, it's possible to mimic a MAC address.

- Want to find your MAC address? This article on Wikihow.com tells you how.

Safer Wi-Fi checklist

On your router:

- Change the administrator password (use a strong one!)
- Enable WPA or WPA2 encryption (WPA2 is best)
- Disable:
  - WPS
  - WAN/Web administration
  - UPnP

SUPERCHARGING YOUR ROUTER

If your router doesn't support the features mentioned in this section, and you like a challenge, you still might be able to "supercharge" it with free, open source firmware like DD-WRT and Tomato. Check their sites to see if your model is compatible.

NOTES

6: Safer chat and voice communication

Making your instant messages, chats and interviews private.

Having a conversation through an unprotected instant messaging or chat program is like having a conversation with someone on a speaker phone in the newsroom: Your colleagues nearby may not know what number you dialed to start the call, or who you are talking to, but they can hear everything that is being said. Online, someone at your ISP may not know your username and password for your chat application, but they see your conversation – with your editor, with a confidential source -- flowing through their network and can log it for later. As a journalist, you may want to keep your interviews more private than that. Here are ways to improve the privacy of your live communication:

The Basics

Use HTTPS

If you chat in your browser — for example, with Google's chat feature, you may already be using HTTPS, which means that your connection to Google's servers is encrypted (though the contents of what you write or say are visible to Google, of course).

Surprisingly, many popular instant message applications only provide a secure connection during your login, but not during your chat.

Use Pidgin with OTR

Pidgin is a free application that lets you put multiple accounts — including Facebook, Yahoo! Messenger, MSN Messenger and Google, in one place. That's a benefit in itself if you have trouble keeping track of who's online, but Pidgin users also can install a plug-in called OTR (Off the Record) that makes chats between Pidgin users more secure: Set up properly, Pidgin with OTR encrypts what's written in an instant message before sending it out across the Internet and won't allow it to be decrypted until it's received by a PC (presumably your source's or a friend's) that has unique permission to read the note. While it's a little more work than chatting in your browser, it's much more secure as it prevents even your chat service provider from being able to read your notes.

As of this writing, Pidgin only supports instant messages and not voice communication. Google reportedly intends to add encryption to its popular GTalk application in the future.

IS SKYPE SECURE?

The developers at Skype, the popular chat and VOIP (Voice Over Internet Protocol) service, say their application provides end-to-end encryption for people participating in a conversation. That means that what you say is encrypted on your PC or mobile device before it's sent over the Internet, and then gets decrypted on the receiving device. While the source code for the program is proprietary and the method has not been independently confirmed, as of this writing there haven't been any recorded incidents of Skype's encryption being cracked successfully.

- Download Pidgin
- Download the OTR plug-in
- Then follow a step-by-step explanation on the Security in-a-Box website to get started with Pidgin and OTR

If you share a PC:

You can download a portable version of Pidgin from PortableApps.com, or a similar version from the developers that has OTR pre-installed, so that you can carry it with you and always have the ability to encrypt your instant messages with you.

But be careful when putting any application on a flash memory stick drive that contains your passwords. Losing the flash memory stick, then, compromises your accounts. If you plan to use Pidgin Portable with your chat accounts, read about using TrueCrypt to lockup your data on the flash drive first.

- Download Pidgin Portable (only)
- Download Pidgin Portable with OTR pre-installed
- Learn about more portable applications

ERASING YOUR CHAT HISTORY

Skype and other Instant Messaging applications save your chat history by default on their servers. You may wish to disable this feature to protect your conversations and contacts in case someone else gets access to your account in the future.

Also, if your application supports video, you may want to check if you are giving permission to share your PC's screen or broadcast a video image automatically. In Skype, these controls are found under the Privacy tab in your Options panel.

Advanced Techniques

Use Tor

You can configure Pidgin to connect to the Internet through Tor for a higher degree of anonymity, though the Tor Project's development team notes that there's potential to leak some information about your identity through your login and password.

- Learn how to configure Pidgin to connect through Tor on the Torporject website (once you reach the page, scroll down a little to see the entry about Pidgin)

SIGNING IN DOESN'T MEAN PROTECTION

While most popular instant messaging programs protect your username and password during sign-in, many do not protect your chat.

More Resources

Front Line Defenders and Tactical Technology Collective

- How to Keep Your Internet Communication Private
- Using Pidgin with OTR — Secure Instant Messaging
- The Digital Survival Guide (for PCs)
- The Digital Survival Guide (for mobile phones)
- Portable Security

Electronic Frontier Foundation

- HTTPS Everywhere

Mobile Active

- Secure Chat on Android: Gibberbot, a User Guide

Skype

- The Skype Security Blog

Chat and Voice checklist

On a PC:

- Download Pidgin and install
- Download the OTR plug-in and install
- Read the instructions for adding an account here
- Read the tutorial for setting up a protected chat with your friends on the Security in-a-Box website
- If you need anonymity when you chat, learn what settings you can use with Pidgin and Tor

If sharing a PC:

- Download Pidgin Portable and install it to a flash drive
- Download the OTR plug-in for Pidgin Portable and install it
- Read the instructions for adding an account
- Read the tutorial for setting up a protected chat with your friends on the Security in-a-Box website
- If you need anonymity when you chat, download the Tor Browser Bundle and then learn what settings to change in Pidgin so that it uses the Tor network

7: Reaching blocked websites

Getting around common road blocks when you try to reach the websites you need for work.

If you frequently do research for your stories onine, you may have been frustrated to find that some sites that are crucial to your subject can't be accessed. There are plenty of reasons this can happen – media companies in several countries restrict content by geographic location for commercial reasons; ISPs may block websites of competitors or websites with mature content (while other ISPs in the same country do not); governments may block websites for cultural or political reasons.

Whatever the reason, you still have some options for accessing blocked sites or content in order to gain a fuller understanding of your story. You can find a thorough review of these (plus some plain talk about what each method does) at the How to Bypass Internet Censorship website, but here are some highlights:

The Basics

First, a word of caution

Try to determine why a website is blocked before accessing it. In some countries, there may be laws that prohibit viewing the site, and breaking these may have consequences for both you and your news organization. If you need to access a website that you already know is blocked in your area, don't try accessing it from a connection that is tied to you: There may be surveillance on the site and someone may be logging the addresses of people trying to access it.

Know the laws

It's important to know the applicable laws in your country when you encounter blocked websites to understand if the content has been banned. Our advice is intended to help facilitate your work as a journalist only.

Use a secure proxy

If you live in an area where websites are frequently blocked, you may have already heard about proxies – services that can "unblock" a site when you connect to the Web through them. Most proxies are *Web proxies*, services that run in your browser and don't require any special software to access them. Many of them are free, but it's good to keep some guidelines in mind when using one:

- Only use proxies that support HTTPS (in fact, using one that provides only an HTTP connection can be disastrous, as your online behavior will be completely visible to your local ISP and anyone else who may be paying attention)
- Don't assume that a proxy service wants to protect your privacy. An HTTPS connection to the proxy is only secure between your PC and their server. After that point, your traffic may be unencrypted and visible to the staff of the proxy service
- Don't provide a proxy service with personal or identifying information when you sign up. The privacy policies of Web proxies differ, and some collect data such as usage habits or email addresses which they then sell for revenue

One proxy service that is free and only requires that users remember an IP address in order to use is called Psiphon. Due to its popularity, Psiphon servers are sometimes blocked in countries that enforce bans on websites. You can receive updated server addresses from the service, however, when you first sign up for an account.

You may wish to use an anonymous email account for your correspondence with Web proxy services, VPNs and the like.

Anonymize with ease

Tails is a self-contained operating system, browser and chat client that is pre-configured to use the anonymizing Tor network — and it even runs from a CD or flash memory stick!

Use a cached link

If you use Google as your search engine, you might see links that say "cached" next to some of your results. Cached versions of pages aren't live — they're images of pages that are being kept on Google's servers to help speed up search results. There's another benefit for users: Sometimes, a cached page won't be blocked, even if the domain of the real website is.

Use a VPN or Tor

- If a website is unavailalbe for any reason in your area, then a secure connection to a VPN in another country, or a connection through the Tor network, might help you climb over the "firewall." Sometimes, a VPN can be faster than Tor, but it's important to remember that a VPN does not provide anonymity – the administrators of the VPN know as much about you as your ISP would if you were not using a VPN.
- Learn about Psiphon 3, a free VPN solution, by sending a blank email to **get@psiphon3.com**
- Learn about OpenVPN, also a free application
- Download the Tor Browser Bundle

Use an RSS Reader

Online RSS readers and other applications that pull in content from different websites, like iCurrent or Google News, may be able to display stories, photos and other content from blocked websites because they aren't blocked themselves.

- Find out how to add topics to Google News
- Learn how to get started with Google Reader
- Learn about iCurrent, a web service that can also send you summaries of stories in email

Know privacy policies

Web proxies and VPN services have privacy policies and it is worth your time to read them. You may discover that your email or other information is shared with other vendors for business purposes.

If you share a PC:

As we've mentioned in the **Safer Surfing** section, you can use the portable Tor Browser Bundle to surf anonymously on the Web if you share a PC in the newsroom or at a local IT café. If you are able to reboot the PC you share without losing access to your network, however, you may be interested in trying Tails, a portable solution that provides an operating system, a browser and instant messaging client pre-configured to work with Tor (which is enabled by default).

If you already have an account with a VPN service, like RiseUp.net's free offering, you may be able to use the portable OpenVPN client to use it, but you also may need a user account with administrator privileges on the PC you use in order to make it work properly. Also, keep in mind that VPNs, like secure proxies, are not designed to provide you anonymity online even if they protect the nature of what you're doing online from your local ISP.

- Get Tor Browser Bundle
- Learn about Tails
- Get OpenVPN Portable
- Learn about other portable security applications

Advanced Techniques

A more thorough list and explanation of circumvention tools — applications that can help users to circumvent firewalls — is available at the How to Bypass Internet Censorship website.

More Resources

How to Bypass Internet Censorship.org

- Quick-Start Guide (pdf)
- Simple Tricks
- Handbook (pdf)

Front Line Defenders and Tactical Technology Collective

- How to remain anonymous and bypass censorship on the Internet

Freedom House

- Leaping Over the Firewall: A Review of Censorship Circumvention Tools

Reporters Without Borders

- Handbook for Bloggers and Cyber-Dissidents

Electronic Frontier Foundation

- How to Blog Safely (About Work or Anything Else)

Global Voices

- Anonymous Blogging with WordPress and Tor

The Internet Censorship Wiki

- Steps to bypass Internet Censorship

Mobile Active

- How to Browse the Web Anonymously on Your Phone

Blocked content checklist

On a PC:

- If you wish to remain anonymous when you surf the Web, as well as reach content that may otherwise be blocked, download the Tor Browser Bundle
- If Tor is blocked in your area, you can try to use a Tor bridge or try a free VPN application
- If you choose to use a VPN, read the instructions for correctly using or configuring it:
  - Riseup.net
  - Psiphon 3
  - HotSpot Shield

If sharing a PC:

- If you wish to remain anonymous when you surf the Web, as well as reach content that may be blocked, download the Tor Browser Bundle
- If Tor is blocked in your area, you can try to use a Tor bridge or try a portable VPN application
- If you choose to use a portable VPN, read the instructions for correctly using or configuring it:
  - Riseup.net (You will also need OpenVPN Portable)
  - Psiphon 3

NOTES

8: Safer social networking & blogging

Knowing what you are sharing in your social networks and blogs.

Facebook, Twitter and other social network sites have become powerful tools for journalists: Media organizations can use them to research information, to find sources or contact witnesses, gather feedback from their audience or crowd-source opinion, or promote their content.

Like any significant outlet for expression, however, these "micro-blogging" services can be monitored, and the results can have consequences for you or for your sources. For instance, if someone had access to your account, they might:

- Copy your list of contacts
- Publish fake content, such as posts that appear to come from you, in order to discredit you or your organization
- Identify an "anonymous" blog (a blog you write under a pen name) through the less-anonymous services or email addresses you may have associated with that blog

Even without access to your account, someone may be able to determine where you were located when you updated your posts using a free tool like Creepy. The following recommendations may help you keep your social communication safer:

The Basics

Use HTTPS

When you log into a social network like Facebook, you should always check that the address of the sign-in page is what you expect and that it is protected with HTTPS. If you have installed the add-on called Perspectives in your browser, you can also check if the site's credentials appear to be authentic. (See our **Safer surfing** section for more about Perspectives and other security add-ons.)

UNUSUAL ACTIVITY? FACEBOOK TESTS IT.

Facebook checks your online habits and asks you to confirm your identity when it spots something unusual.

Some sites support HTTPS connections throughout your session, which can prevent your ISP and people who share your network from monitoring what you post or online conversations you have during your session. Facebook and Twitter both let you enable this feature in their Account Settings.

- Learn how to enable HTTPS connections in Twitter
- Learn how to enable HTTPS connections in Facebok

Use a strong password

As with any Web service, you should follow recommended practices when you set up your password and password recovery plan for a social network. This is especially important for news organizations and bloggers who use Facebook and Twitter to interact with their audience, as losing control of an account can damage a hard-won reputation.

- Review recommendations from the Security in-a-Box website for making a strong password

Use a VPN or Tor

A Virtual Private Network (VPN) can provide increased privacy when you surf the Web, and this includes your use of social networks. As a reminder, though, a VPN only provides privacy between yourself and the VPN service provider. The Tor Browser Bundle can provide anonymity between your PC and the website you are accessing, but you'll still want to make sure your connection to the site is through HTTPS to prevent unintentionally sharing your posts with people in the Tor network.

- Download the latest version of the Tor Browser Bundle
- Learn about Psiphon 3, a free VPN solution, by sending a blank email to **get@psiphon3.com**

Turn on 2-factor verification

Your social network site or blog host might give you the option to protect your user account with more than just a username and password to sign in. Facebook, for instance, lets you protect your account by also requiring a code sent to your mobile phone (you'll find it under Account à Account Settings à Mobile). See if the social network sites you use support a similar feature.

- Learn how to add 2-factor verification for Facebook
- Add 2-step verification for all Google accounts

Keep it anonymous

Reporters Without Borders (RSF) and the Electronic Frontier Foundation (EFF) have produced manuals with tips for bloggers, including how to blog anonymously. The same habits are useful , though, for journalists who, for whatever reason, wish to protect their identity when posting online:

- Get RSF's "Handbook for Bloggers and Cyber Dissidents"
- Get EFF's "How to Blog Safely (About Work or Anything Else)"

Know what you are sharing

The privacy policies on social networking sites change frequently and you may find that information that was limited to a small circle of people you invited yesterday is suddenly available to the general public today. Additionally, networks are getting more invasive in inspecting what we post, though often with good intentions. Facebook, for instance, has adopted the practice of monitoring key words and phrases in conversations and posts to spot illegal activity that may put some members at risk. Make it your business to know the privacy policy of the social network you use so that you also understand what information about your account – and your contacts — is being shared with strangers.

- Learn how you may be sharing information you aren't aware of through your use of social networks

Similarly, be aware that when you write or post anything to a blog or social network page that is connected to your real identity, you are also alerting people to what you are following in your local area. In Mexico, drug gangs have sifted through posts in profile pages in Facebook to track down and kill citizen journalists reporting on gunfire in small towns.

Mobile phones

Mobile phone users may benefit from additional recommendations from Mobile Active, an organization that deciphers mobile technology for activists (and other users):

- Learn how to make Facebook safer
- Learn how to make Twitter safer

While smart phone users are subject to the same safety concerns as PC users when using social network websites, they should also keep in mind that online crowd-sourcing platforms such as Front Line SMS and Ushahidi – depending on how they are used – can expose information about users that would normally be available only to a mobile service provider.

Protect passwords everywhere

Don't keep passwords for your social networking sites unprotected on your phone.

WHERE HAVE YOU BEEN?

When you post to social networks, you may be sharing more than just your thoughts or a quick news report. Some additional information, like your location, also may be available. The free application **Creepy**, for instance, lets someone type in a Twitter username in order to find out where that was when they posted their tweets.

More Resources

Front Line Defenders and Tactical Technology Collective

- How to Protect Yourself and Your Data When Using Social Networking Sites
- Portable Security

Facebook Safety Center

- Facebook's safety tools

Safer social networks checklist

On a PC:

- Start by reading the recommendations from RSF and EFF for blogging safely. The same information will be useful for using social network sites
- Whether using an existing account or creating a new one, make sure you use a strong password. You can read more about strong passwords on the Front Line Defender's Security in-a-Box site
- Enable HTTPS connections to your social network sites, if that feature is available. Both Facebook and Twitter support this under Account Settings
- Use a VPN or Tor to improve your privacy

If sharing a PC:

- Use a portable VPN and browser or use the Tor Browser Bundle
- Check the shared PC for malware that might record your activity
- After posting, run portable CCleaner to remove traces such as your browsing history and temporary files on the PC

On a smart phone:

- Read Mobile Active's user guides for:
  - Tor on your phone
  - Safer Facebook
  - Safer Twitter

NOTES

9: Really delete your data

Making sure you are really deleting the files you don't want on your PC or smartphone.

Did you know that, when you delete an old article, photo or interview clip from your PC, it might not really be deleted?

It's true. When you Empty Recycle Bin in Windows, for instance, you're just telling the PC that it's okay to write new data on top of the old – and until that actually happens, you or someone else may be able to retrieve what you thought was safely thrown away.

This is also true of flash memory sticks and mobile phones. If you accidentally delete a picture on your phone (or if someone forces you to do it), you may be able to retrieve the photo/data later with Recuva or other free recovery applications.

Programs like Recuva examine the parts of your hard drive where data has been "deleted" to put the pieces back together. As useful as that is when you accidentally delete that perfect photograph from your camera's SD card and need to get it back, it can also be unnerving to see how many files you are unknowingly storing on your PC, phone or flash memory stick.

Those files could be anything, of course – notes from interviews, addresses of your sources, old email—and, in the event that your PC is seized or stolen, there's a high likelihood that the people involved will use some type of data-retrieval software to scrub every last sector of the drive for those things. Don't believe it? Download Recuva to see what may be lurking in the shadows of your Windows PC right now.

- Download Recuva to see what is "deleted" on your PC or device

WIPE IT BEFORE YOU GIVE IT

If you plan to sell, donate or lend an old PC to someone, you should wipe the hard drive securely first, deleting everything. A free utility called Darik's Boot and Nuke – or DBAN for short, is perfect for that sort of task.

The Basics

Use Eraser

Free applications like **Eraser** don't just delete a file: They immediately write random bits — ones and zeroes — on top of it, making it much more difficult to retrieve. This form of deletion takes longer than just emptying the Recycle Bin, but it's worth the extra effort, especially if you have confidential sournces whose safety may depend on your discretion.

- Download Eraser to be able to delete sensitive files permanently
- Learn how to use Eraser at Security in a Box website

Use CCleaner

CCleaner is great at removing the most common traces left on PCs, such as your Web history, which makes it an invaluable tool for anyone who shares a PC in the newsroom or who blogs from a public IT café. But it can also use the same method of deletion that Eraser uses when it cleans out your cache and other cyber trash.

- Download CCleaner so you can delete your Recycle Bin files and other cached files permanently
- Learn how to configure CCleaner to delete files securely from Front Line Defenders and Tactical Technology Collective's Security in-a-Box website

ERASING FLASH DRIVES, SSDS AND MEMORY STICKS

Flash drives, including solid state drives (SSD) and memory sticks, don't store data or erase data the same way as a spinning hard drive. If you need to wipe an SSD, make sure you use a secure deletion tool provided by the manufacturer on their website. If you are wiping an entire flash memory stick, be sure to check that your data is completely destroyed with Recuva before considering the operation successful.

Be Proactive!

Okay, we admit that this isn't strictly a method for deleting files, but it's worth pointing out that what you write on the Web stays on the Web — and you might not be able to delete it.

- The US Library of Congress is currently archiving every tweet ever uttered on Twitter for posterity
- The Internet Archive, launched in 1996, maintains hundreds of thousands of websites, audio files, video clips and public domain books
- Google keeps snapshots of every page its search engine crawls on its own servers, making them available even if the site is no longer live

While this shouldn't cause you to self-censor your work, just keep in mind that immortality — at least on the Internet — is a reality in today's world.

If you share a PC:

You can use a portable version of Eraser or CCleaner on a flash memory stick so you don't accidentally leave "ghosts" of your work on the PC. There's also a portable version of Recuva available, in case a file on your flash memory stick suddenly goes missing.

- Download Eraser Portable to carry Eraser with you on a flash memory stick
- Download CCleaner Portable to erase your Web traces, cached files and files in the Recycle Bin permanently
- Download Recuva Portable to recover files you accidentally deleted
- Learn about other portable security applications

More Resources

Front Line Defenders and Tactical Technology Collective

- VIDEO: ONO Robot's Guide to the Traces We Leave Behind
- How to Recover from Information Loss
- How to Destroy Sensitive Information
- How to Use Recuva
- How to Use Portable Eraser

Mobile Active

- Mobile tools for Backups, Data Deletion and Remote Wipe

ERASING FOR ETERNITY

If you use Eraser or other secure deletion program, you may be given a choice of writing on top of your deleted data up to 35 times. That may seem like a lot (and it certainly takes longer than, say, the three times that most experts recommend to evade today's most common data-retrieval methods), but what about tomorrow's methods?

Secure deletion checklist

On a PC:

- Download and install Eraser. In the Settings menu, tell Eraser how many passes you want it to use when deleting an individual file (the default is 35 passes) or when writing on top of old deleted data that may still be hiding in your hard drive's unused space (three passes).
- Do some house cleaning: Launch Eraser (Windows 7 users will need to Run as Administrator for this task), click the Erase Schedule drop-down menu and select "New Task." In the pop-up window, click the "Add Data" button, select "Unused disk space" and click "OK." You should see the task show up in Eraser's main window now. Right click it and choose "Run Now." This will erase any old files that were previously deleted but may still be hiding on your hard drive.
- Download and install CCleaner. Under Options, choose Settings and then enable "Secure file deletion." Decide how many passes you want CCleaner to write on top of your deleted data. More passes will take longer, but that method is also more secure.

If sharing a PC:

- Download portable CCleaner and portable Eraser and install them to a flash memory stick so you can securely delete your files on a shared PC

ONCE YOU LOSE IT, DON'T USE IT

You can improve your chances of recovering data from a drive by not using it once the data has been lost. When you use a drive, it may write new data on top of the old files you want to recover.

10: Respecting the risks of sharing data online

Using file-sharing services, like Dropbox, safely.

One of the most useful trends of the Web has been the move to the Cloud — putting data onto public servers so that you can share it more easily with other people or store it for your own use. Journalists who work on their stories from multiple locations and who use multiple devices no longer need to carry their files with them — it's all in the Cloud. Collaboration on stories that previously required fancy servers and a tolerance for technical headaches is now so easy we wonder why someone didn't think of it sooner.

The benefits are undeniable: Services like Google Docs let a group access the same files online, collaborate and avoid constant emailing. File-sharing services like Dropbox provide a free or cheap way to back up your files to a remote location.

But sharing data online also brings some risks of exposure that are worth keeping in mind if you would like to help you use these services wisely.

For instance, a shared folder on the Internet is only "private" as long as all of its members keep their passwords safe and don't lose control of their computers. Otherwise, the addresses of all users of a shared folder may be exposed — in addition to the contents of shared folders. Even when a folder is kept private, its contents may be accessible to the service providers' employees or someone who has accessed their servers. (Mat Honan, in an article in *Wired*, explained how hackers were able to gain access to his iCloud account and use this to delete data on his laptop and linked mobile devices.)

Mobile users accessing a shared web service — for example, one that allows you to post short comments on a webpage via SMS — may also be sharing location and identity information.

DROPBOX SECURITY

Dropbox uses HTTPS connections between your PC and its servers, and encrypts your files once they have been uploaded, though the company says it does have access to your password. The company announced in August 2012 that it is adding 2-Step Authentication to its service soon.

Also, cloud storage can sometimes have drawbacks: Mat Honan, in an article in *Wired*, recently explained how hackers were able to gain access to his iCloud account and use this to delete data on his laptop and linked mobile devices.

The Basics

Use HTTPS

Dropbox, Google Drive and some other file-sharing services enforce HTTPS connections by default. Make sure that yours does so that the traffic between your PC and the online service you use is protected.

Review who has access

If you manage or "own" a shared folder, take a moment to review the people who have access to it. Does everyone still need access to all the files? If the folder was related to an investigative story that your news organization published last year, for instance, does it need to remain online? Set reminders for yourself to review permissions for your folders every few months. You may also wish

to do "house cleaning" to confirm that you still want the files currently online to remain there.

Use encryption

Dropbox encrypts your files *after* they have been uploaded, but retains your encryption key (your password) in case law-enforcement agencies require them to provide access to users' data.

Some services, such as SpiderOak, encrypt your data on your PC *before* it is uploaded and do not retain your password, a method that prevents a company from revealing your data even under court order.

What's important, however, is that you not rely on your file-sharing service alone for privacy. If your data is sensitive, encrypt it before you upload it. TrueCrypt, a free encryption application, is one way to create encrypted folders that you then can upload to your file-sharing service.

PROTECT YOUR FILES IN THE CLOUD

You can use an encryption program like TrueCrypt (www.truecrypt.org) to protect the files you intend to store in the Cloud with a password.

Use a VPN or Tor

If you access Dropbox or other file-sharing services **through a browser,** you may want to use a VPN or Tor to avoid making your habits public. Keep in mind, however, that *it is essential you maintain an HTTPS connection* with the service you are accessing unless you wish your activity to be exposed to the VPN's staff or to someone on the Tor network.

If you share a PC:

While portable versions of Dropbox are in development, you may be better off accessing Dropbox through a portable browser that you control.

This recommendation applies to other online file-sharing services, as well. If you're not using Tor Browser Bundle, which comes with a portable browser built in, you can:

- Download Firefox Portable
- Read about security Add-Ons that can improve your privacy when using Firefox
- If you require anonymity, download the latest version of the Tor Browser Bundle from Torproject.org to improve your local privacy and anonymity on the websites you visit

DON'T MAKE YOUR PASSWORDS EASY TO FIND

Don't keep passwords for your file-sharing service unprotected on your mobile device or, for that matter, on a piece of paper taped somewhere on your desk or computer monitor!

- Make sure your service provides a secure connection to its servers, for instance through HTTPS (SSL)

Anonymous sharing

File-sharing services are great tools for collaborating on projects with colleagues, but you may wish to provide a way for sources to anonymously leave information for you – a sort of "dead drop," where you can receive tips and other information anonymously.

The notoriety of Wikileaks has led some developers to seek ways to create similar services for whistleblowers, including Globaleaks and Gitorious. Separately, **Tor2web.org** has attempted to make it possible for users to anonymously publish to the Web.

You can also find an impressive list of existing dead drop services — services that let you upload files for another person to pick up later and that do not maintain server logs — for whistleblowers at LeakDirectory.org.

More Resources

- Get more recommendations from DrawingByNumbers.org on what to consider when you share content
- Handbook for Bloggers and Cyber-Dissidents (Reporters Without Borders)
- How to Blog Safely (Electronic Frontier Foundation)
- Anonymous Blogging with WordPress & Tor (Global Voices)
- Portable Security (Security in-a-Box)

Safer Cloud checklist

On a PC:

- Start by reading the recommendations from Reporters Without Borders (RSF) and the Electronic Frontier Foundation (EFF) for blogging safely. The same precautions may be useful when creating file-sharing accounts
- Whether using an existing account or creating a new one, make sure you use a strong password. You can read more about strong passwords on the Front Line Defenders and Tactical Technology Collective's Security in-a-Box website

- Check your file-sharing service's website to confirm it provides connections (for instance, through HTTPS). If your service doesn't provide a secure connection, move on to one that does
- If you wanted to use your file-sharing service through a VPN or Tor, be aware that you may need to configure your application to use these services

If sharing a PC:

- You can still use a file-sharing service on a shared PC through a browser. Follow best practices for passwords, using a strong one, never saving it on a shared PC and deleting your temporary files with a utility like CCleaner when you are done
- Confirm that your online file-sharing service enforces a secure connection through HTTPS
- Check the shared PC for malware that might record your activity
- If additional privacy is essential, or if file-sharing services are restricted in your area, you may be able to use a portable VPN and browser, or the Tor Browser Bundle, to access them

NOTES

11: Safer cellphones

Safely use your mobile device for multiple tasks.

As cell phones have grown smarter and the networks they use increasingly ubiquitous, we've happily embraced them as a tool of work. Today's phones do many of the tasks that previously only a PC could handle, letting us post to social networks, browse email, edit photos or audio clips and conduct research all from the comfort of our palm. No other category of device is helping more people in more places to access more information. Oh, and they make calls.

It's important to understand, though, that information access works both ways: Your phone, with its lists of contacts, recent phone calls and SMS messages, perhaps records of your Web activity and even your physical location, can tell a perfect stranger a lot about you both personally and professionally, and maybe more than you intend.

At the same time, your cell phone service provider may keep track of a range of data related to customers for billing and other purposes, including location, SMS messages and when they were sent, when calls were made, and so on.

Depending on the provider, that information may be shared with other companies. And, as service providers are subject to the laws of the countries in which they operate, that same information may be shared with authorities and, by extension, the authorities of other governments with whom they have agreements. (You can learn much more about how cell phones work and the most common risks associated with them, at *SaferMobile's Mobile Network Awareness: The Basics* or Tactical Technology Collective's Mobile Devices and Security.)

While there are some ways to protect the data on your phone and some Internet activities that we'll describe here, it's important to remember that your voice phone calls and SMS messages are transparent to your service provider and anyone else who might have the equipment or know-how to access them.

SECURE ACCESS TO YOUR PHONE

You should always enable strong passwords on your smartphone to protect your data in case the device is lost or stolen.

Hang onto it

One of the strengths of cell phones is their size: They deliver a lot in a convenient package. That can also make them easy to lose, and can make them easy targets for theft and confiscation. Lookout, a mobile security firm, estimates, "Everyday, (US)$7 million worth of phones are lost by Lookout users alone." So keeping your phone in your possession is a priority.

Make it hard to unlock

In the Protecting Your Data section, we reviewed the benefits of using strong passwords to keep information on your device private. The same is true for cell phones.

Many phone operating systems, including Android, Blackberry and Apple's iOS, let you create passwords that are longer than just a four-

digit code and that can have special characters and numbers mixed in. (Visit the appropriate manufacturer's website for instructions.)

Also, some phones, such as Blackberry devices and phones with Android 4 or higher, have a built-in encryption feature for data on the phone, which makes protection more complete if someone has physical access to the phone. If you use iPhone, a third-party application like Wickr may be able to provide this protection, as well. Check your manufacturer's home page and app outlet for encryption features available for your make and model.

- Get more tips about creating strong passwords from the Security in-a-Box website

LIMIT THE ATTEMPTS TO UNLOCK IT

Some smart phones lock when an incorrect passphrase has been typed several times. Read the instructions for your model to see if this feature is available to you

Make data disposable

If you are concerned that your phone may be confiscated at any time, regardless of the precautions you take, you may wish to keep sensitive data such as contacts and photos on a flash memory card (e.g. microSD) that can be removed from the device and disposed easily.

Not all phones have flash memory card slots, however. In those cases, you may wish to consider saving the data you feel is most sensitive on the phone's SIM card, which can also be removed and destroyed, albeit not very quickly.

Save and protect backups

As described earlier in Protect Your Data, you should always keep more than one copy of your data safely tucked away — one nearby and one at another location, to protect against natural and man-made disasters.

Some phone makers provide backup software that syncs your data to a PC and encrypts it along the way. If your phone does not include a special application that supports encryption, you can still protect your backups by saving them to an encrypted folder on a PC or on an external drive that you make with a computer application like TrueCrypt.

Just as with PCs, you can use calendars or other ways of reminding yourself to update your backups on a regular basis.

- Learn more about TrueCrypt at the developer's website
- Visit the Security in-a-Box website for a TrueCrypt tutorial

Make your connection more private

The Guardian Project has developed a trio of privacy applications for Android users — Orbot, Orweb and Gibberbot — that can provide a high degree of anonymity for people who use their Android phone to surf the Web or chat.

In the case of Web surfing, Orbot with Orweb has the additional benefit of making some websites available that were not available through a regular browser, though please see our section on Reaching Blocked Websites to understand some of the issues surrounding this.

Just as with the computer application Pidgin (with the OTR plug-in) described in the Safer Chat and Voice Communication section, the Gibberbot instant message application lets two users who "authenticate" one another create an encrypted chat so that the text is not visible to service providers or others in-between. On the iPhone platform, Wickr can provide encryption for the content of instant messages sent to other Wickr users, though it doesn't provide anonymity. While Blackberry was a pioneer in providing encrypted chat services, there has been some concern about their policies and participation in surveillance projects.

- Learn how to use Gibberbot in a tutorial from Mobile Active
- Learn more about Gibberbot at The Guardian Project
- Read MobileActive's instructions for browsing the Web anonymously with Orbot

Some Web services, like Facebook and Twitter, have made it easy for us to access their services through small applications on our smart phones, though our privacy may not have been their primary concern. MobileActive offers some easy recommendations in making use of each service a little safer:

- Learn how to make Facebook safer
- Learn how to make Twitter safer

Be aware of what you install and what your apps have access to

Before you install an application on your cell phone, it's worth taking a moment or two to make sure that you need the application, that the application is exactly what you think it is, and that it doesn't require higher access to information on your phone than you feel comfortable with.

Just as you might do when downloading an application for a PC, you might wish to check user reviews and other resources before you install any application on the phone.

Install some armor

While viruses and other malware are still relatively rare for mobile users, they are becoming more common as smart phones become more popular. Most large anti-virus companies now make mobile versions of their applications that come with firewalls, though sometimes these programs are not free. Android phones that run any version of the operating system higher than 4.0 have an encryption feature included — just navigate to Settings –> Security and lock screen to get started. Earlier versions of Android can use DroidWall, available in the Google Play market, but installation can be tricky since it requires root access to your phone.

- Learn more about DroidWall on its developer web page

What if the worst happens, anyway?

My phone was taken!

If your phone has been stolen or confiscated, there isn't much you can do unless you have taken steps prior to losing control of the phone:

- If you have configured your phone to use a remote-wiping feature, use it immediately. Remote wiping allows you to send a code to your phone that instructs the device to delete all the data on the phone
- Change the passwords of any accounts you had synced to the phone, such as email, Facebook or Twitter accounts
- Review the results of your initial risk assessment: If someone decrypts the information on your phone, seeing your contacts, call logs, SMS Inbox, photos and any other data, who is put at risk, how and to what extent
- Notify people who may be affected by the loss of the phone

I think my calls are being recorded!

If you believe that your mobile phone is tapped and your calls are being recorded, there are a couple of steps you can take that may help, temporarily:

- First, review Mobile Active's recommendations for dealing with surveillance, as well as Security in-a-Box's recommendations for Best practices for phone security
- Turn off your compromised phone and remove the battery
- Purchase a new handset and SIM card (it is essential that you do both, as each component has its own identification number. Just replacing your SIM card won't provide you a new identity if the handset is already associated with you, as well)
- Before you put a battery in the new phone: Be aware that it is possible to track the location of a phone whether you are using it or not, and **whether it is turned on or off**. Taking the new phone to your home or place of work will associate the new phone with those locations
- Leave the battery out of the phone until you intend to use the phone for calls. When you are finished with calling, remove the battery. You may wish to alert your colleagues and friends that the phone will be available during specific hours, and plan not to be at your home or place of work during those hours
- Purchase a new SD card
- Using a PC, copy the contacts from your old SD card to a new one. Do not transfer applications

More Resources:

MobileActive:

- A User Guide to Orbot — Anonymized Tor Browsing on Your Mobile Phone
- Safer Facebook
- Safer Twitter
- Mobile tools for Backups, Data Deletion and Remote Wipe

Security in-a-Box:

- How to use mobile phones as securely as possible

Safer Cell Phones Checklist

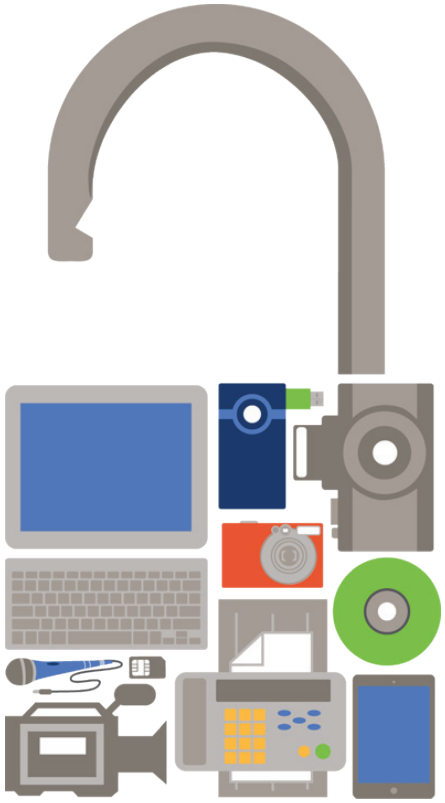
Always lock your phone with a password or PIN. If your phone supports a password that is longer than a four-digit PIN, enable this feature. Get in the habit of keeping the phone locked whenever you are not using it

If your phone has a built-in encryption feature, as Blackberry and Android devices do, make sure it is enabled. If you have an iPhone, a third-party application like Wickr may provide the same functionality

Some smart phones lock when an incorrect passphrase has been typed several times. Read the instructions for your model to see if this feature is available to you

Pick a method for backing up the data on your phone try to regularly save your data, and protect it with encryption

12: Applying "safety first" to other technologies



Not-so-smart devices like fax machines and cameras have safety concerns, too.

As you become more aware of the challenges of online safety and adopt some new, safer habits in your work as a journalist or blogger, you may want to apply your knowledge to other technologies you use besides a PC or smart phone. Here are just a couple examples:

Faxing

Journalists who use a fax machine should consider the following:

- If you are asked to provide your name or address when you send a fax, agree in advance to a pen name with your editor or source and use that name
- Re-collect your pages as they go through the fax machine. Never leave the documents you have faxed in the shop

Photos and video

The digital pictures you take carry a lot more information than just the images. Hidden in the *metadata* — the information that is automatically embedded in each picture — you may find date and time stamps, the type of camera used and, more and more frequently, the GPS location where the photo was taken. Video files also may contain metadata. An application like Irfanview can display and help you delete this sort of information on your PC.

If you are concerned that a particular photo or video you intend to publish may be traced to you, you should learn how to remove this information and how to safely handle the upload. Android phone users should investigate ObscuraCam, an application developed by the Guardian Project and Witness.org that lets users pixelate (and hide) the faces of specific subjects in their images, all done in-camera.

INFORMATION BEHIND YOUR PHOTO

IrfanView (www.irfanview.com) is a popular, free photo editor that can show you what "hidden" information your photos may contain.

Here are some more resources:

- Learn how to remove location information from your pictures from Mobile Active
- Find IrfanView plug-ins for video
- Get tips from Small World News on how to produce media securely
- Learn about ObscuraCam for Android, or...
- Download ObscuraCam from Google Play

Your PC's camera and microphone

In early 2009, researchers discovered a Trojan virus they called GhostNet that, among other things, gave hackers remote control of the cameras and microphones on infected PCs, presumably to use for spying. It's been identified in more than 100 countries.

In February 2012, a flaw in TrendNet-brand webcams was discovered that allows people on the Internet to detect and then access the "private" feeds of thousands of camera users.

The point? The camera and microphone on your PC may be on when you don't know it. How you feel about that is your business, but you should know that Windows lets you uninstall the software that drives the camera and microphone on your laptop -- essentially turning it off. (Go to Start and "Device Manager," find your devices among those listed, right click them and choose Uninstall from the options.) And, of course, there's always the old-fashioned method of putting tape over the lens.

INTERNET SAFETY PODCASTS

You can learn more about Internet safety and daily threats from podcasts such as Security Now! and SANS Internet Storm Center.

NOTES

13: What to do if...

First Aid for an infected PC, a hacked account and other emergencies.

The Internet and our phone networks weren't designed with security in mind, and it's difficult to avoid risks to your devices even when you take precautions. Here are a few things you can do if the worst happens:

My PC is infected!

- Update your anti-malware applications
- Disconnect the PC from the network
- Restart the PC in Safe Mode (on most PCs, you enter Safe Mode by pressing F8 during reboot, but check your user manual for your particular model)
- Scan the PC, making sure you have selected "Full Scan." (Some of your anti-malware applications may not run in Safe Mode, but start with those that do. Then reboot your PC normally to run scans with the remaining programs.)
- If you have a clean bill of health or you found malware and have removed it, get a second opinion:
    - Run an online scanner like HouseCall, or...
    - Run an offline scanner like Microsoft's Safety Scanner, AVG's Rescue Disk or Comodo's Cleaning Essentials
    - If you use Windows, consider running a diagnostic tool like Hijack This to reveal all the processes running on your PC. Because Hijack This doesn't distinguish between "good" and "bad" processes, you should post your results in a forum, or use an online tool like Hijackthis.de to help decipher what you are seeing before you try deleting any files

ARE YOU REALLY FREE OF MALWARE?

Once a PC is infected, it's very difficult to confirm that it is free of malware, even if your anti-virus application says so. Hackers frequently write their viruses to avoid detection and they're good at what they do. You may need to wipe your hard drive and reinstall your operating system and programs.

- If you are still infected, you need to consider...
- Reverting to an earlier "snapshot" of your PC's hard drive — see our section on backups to learn how
- Wiping your hard drive with a specialty program like DBAN (Darik's Boot and Nuke), and then reinstalling your operating system and programs

My PC won't start!

If your PC won't boot or consistently crashes during the start-up process, there may be several potential causes, and you may need an expert to repair the computer.

If that happens:

- Locate your backups so you can work on another PC, if need be, while you wait for the repair
- Stay with the person who is helping fix your PC: It's a good opportunity to learn how experts diagnose problems, but it's **essential** that you prevent someone from taking your hard drive and replacing it without your knowledge or permission

- Never leave your PC at a shop unless you have removed the hard drive first
- If your hard drive must be replaced, make sure this is done in your presence and that you keep your old hard drive. If data must be copied from the old hard disk to the new one, make sure this is done in your presence, as well, and that the copy is being made by the PC that is being repaired, and not by a third PC in the shop
- If it turns out that you need someone to recover data from your hard disk, have this done in your presence. Leaving the hard disk overnight in the shop is not an option

REPORT CYBER ATTACKS

Have you been the victim of a cyber attack? You can contact Reporters Without Borders and let them know.

Someone has been using my account!

If you spot suspicious activity on your email or social network accounts, but still have access to the accounts, you should:

- Confirm under Settings that there are no email addresses or mobile phone numbers associated with the account that do not belong to you
- Change the password and security question, following recommended guidelines
- Learn about adding additional protection for your account through 2-step verification
- If you lose access to the accounts, you should:
- Contact your email service provider's support staff and notify them that you suspect your account has been taken over by someone else. Request steps to reset your password
- Create a replacement account with a new password and new security question, following guidelines recommended in other sections of this toolkit
- If your service provider can't help you regain access to the account, notify your friends and colleagues that you suspect your account is being used by someone else. Ask them not to reply to emails or other messages from the account, and to alert you if they see activity. Offer to confirm your current identity by phone, Skype or in-person – after all, how do they know that you are really *you*?
- Using a recent backup of your email, copy your contact lists from the compromised account
- If you use an email client like Thunderbird, copy your offline email from the compromised account to the Inbox of the new one

NOTES

Glossary

The following glossary of technical terms is partially provided under Creative Commons Attribution-Share Alike 3.0 Unported License from the Security in-a-Box website created by Tactical Technology Collective and Front Line Defenders.

Some of the technical terms you encounter in this toolkit are defined below:

- **Avast** – A freeware anti-virus tool
- **Basic Input/Output System (BIOS)** – The first and deepest level of software on a computer. The BIOS allows you to set many advanced preferences related to the computer's hardware, including a start-up password
- **Bitlocker** – an application in Enterprise and Ultimate versions of Windows Vista and Windows 7, is simple to use and can not only lock up your PC, but external hard drives – like those you might use for backing up your data.
- **Blacklist** – A list of blocked websites and other Internet services that can not be accessed due to a restrictive filtering policy
- **Bluetooth** – A physical wireless communications standard for exchanging data over short distances from fixed and mobile devices. Bluetooth uses short wavelength radio transmissions.
- **Booting** – The act of starting up a computer
- **CCleaner** – A freeware tool that removes temporary files and potentially sensitive traces left on your hard drive by programs that you have used recently and by the Windows operating system itself
- **CD Burner** – A computer CD-ROM drive that can write data on blank CDs. DVD burners can do the same with blank DVDs. CD-RW and DVD-RW drives can delete and rewrite information more than once on the same CD-RW or DVD-RW disc.
- **Circumvention** – The act of bypassing Internet filters to access blocked websites and other Internet services
- **Clam Win** - A FOSS anti-virus program for Windows
- **Cobian Backup** – A FOSS backup tool. The most recent version of Cobian is closed-source freeware, but prior versions are released as FOSS.
- **Comodo Firewall** – A freeware firewall tool
- **Cookie** – A small file, saved on your computer by your browser, that can be used to store information for, or identify you to, a particular website
- **Digital signature** – A way of using encryption to prove that a particular file or message was truly sent by the person who claims to have sent it
- **Domain name** – The address, in words, of a website or Internet service; for example: security.ngoinabox.org
- **Domain Name System (DNS)** – A network of servers sometimes called the directory or phone book of the Internet. It translates domain names into IP addresses
- **Encryption** – A way of using clever mathematics to encrypt, or scramble, information so that it can only be decrypted and read by someone who has a particular piece of information, such as a password or an encryption key
- **Enigmail** – An add-on for the Thunderbird email program that allows it to send and receive encrypted and digitally signed email
- **Eraser** – A tool that securely and permanently deletes information from your computer or removable storage device
- **Firefox** – A popular FOSS Web browser that provides an alternative to Microsoft Internet Explorer
- **Firesheep** – A popular add-on for Firefox developed by Eric Butler that allows users to hijack the open sessions of many popular websites over unencrypted connections
- **Firewall** – A tool that protects your computer from untrusted connections to or from local networks and the Internet
- **Free and Open Source Software (FOSS)** – This family of software is available free of charge and has no legal restrictions to prevent a user from testing, sharing or modifying it
- **Freeware** – Includes software that is free of charge but subject to legal or technical restrictions that prevent users from accessing the source code used to create it
- **GNU/Linux** – A FOSS operating system that provides an alternative to Microsoft Windows
- **Global Positioning System (GPS)** – A space-based global navigation satellite system that provides location and time information in all weather, anywhere on or near the Earth, where there is an (almost) unobstructed sky view.
- **Hacker** – In this context, a malicious computer criminal who may be trying to access your sensitive information or take control of your computer remotely
- **Internet Protocol address (IP address)** – A unique identifier assigned to your computer when it is connected to the Internet

- **Internet Service Provider (ISP)** – The company or organisation that provides your initial link to the Internet. The governments of many countries exert control over the Internet, using means such as filtering and surveillance, through the ISPs that operate in those countries.
- **Infrared Data Association (IrDA)** – A physical wireless communications standard for the short-range exchange of data using infrared spectrum light. IrDA is replaced by Bluetooth in modern devices.
- **Java Applications (Applets)** – Small programs that can run under many operating systems and are cross-platform. They are frequently used to provide improved functionalities within web pages.
- **Keylogger** – A type of spyware that records which keys you have typed on your computer's keyboard and sends this information to a third party. Keyloggers are frequently used to steal email and other passwords.
- **KeePass** – A freeware secure password database
- **LiveCD** – A CD that allows your computer to run a different operating system temporarily.
- **MAC address** – The Media Access Control address is a unique identification number associated with individual computers, smart phones and other devices. While they are hard-encoded into a device, it is possible for users to "spoof" (fake) a MAC address and, thereby, appear to be another machine
- **Mac Filtering** – This method of controlling access to your network by the MAC addresses of individual devices does not encrypt or otherwise protect the data sent between a PC and a router
- **Malware** – A general term for all malicious software, including viruses, spyware, trojans, and other such threats
- **Mnemonic device** – A simple trick that can help you remember complex passwords
- **NoScript** – A security add-on for the Firefox browser that protects you from malicious programs that might be present in unfamiliar webpages
- **Off the Record (OTR)** – An encryption plugin for the Pidgin instant messaging program
- **OpenDNS** – A free service (for individuals) that replaces the DNS service of a user's ISP (Internet Service Provider) with a curated one. Can help protect against "man-in-the-middle" attacks if hackers or other people abuse the local DNS routing tables
- **Peacefire** – Subscribers to this free service receive periodic emails containing an updated list of circumvention proxies, which can be used to bypass Internet censorship
- **Phishing** – Creating fake websites or email that appear genuine in order to lure Internet users to interact with the content. Frequently used to capture passwords and financial data.
- **Physical threat** – In this context, any threat to your sensitive information that results from other people having direct physical access your computer hardware or from other physical risks, such as breakage, accidents or natural disasters
- **Pidgin** – A FOSS instant messaging tool that supports an encryption plugin called Off the Record (OTR)
- **Portable applications** – Programs that run from a portable device, such as a flash memory stick or memory card, and do not require installation under the PC's operating system.
- **Proxy** – An intermediary service through which you can channel some or all of your Internet communication and that can be used to bypass Internet censorship. A proxy may be public, or you may need to log in with a username and password to access it. Only some proxies are secure, which means that they use encryption to protect the privacy of the information that passes between your computer and the Internet services to which you connect through the proxy
- **Proprietary software** – The opposite of Free and Open-Source Software (FOSS). These applications are usually commercial, but can also be freeware with restrictive license requirements.
- **Reaver** – An attack tool designed to crack the encryption key used by WPS (Wi-Fi Protected Setup)
- **RiseUp** – A email service run by and for activists that can be accessed securely either through webmail or using an email client such as Mozilla Thunderbird
- **Router** – A piece of networking equipment through which computers connect to their local networks and through which various local networks access the Internet. Switches, gateways and hubs perform similar tasks, as do wireless access points for computers that are properly equipped to use them
- **Secure password database** – A tool that can encrypt and store your passwords using a single master password
- **Secure Sockets Layer (SSL)** – The technology that permits you to maintain a secure, encrypted connection between your computer and some of the websites and Internet services that you visit. When you are connected to a website through SSL, the address of the website will begin with HTTPS rather than HTTP.
- **Security certificate** – A way for secure websites and other Internet services to prove, using encryption, that they are who they claim to be. In order for your browser to accept a secu-

rity certificate as valid, however, the service must pay for a digital signature from a trusted organization. Because this costs money that some service operators are unwilling or unable to spend, however, you will occasionally see a security certificate error even when visiting a valid service.

- **Security policy** – A written document that describes how your organization can best protect itself from various threats, including a list of steps to be taken should certain security-related events take place
- **Security cable** – A locking cable that can be used to secure a laptop or other piece of hardware, including external hard drives and some desktop computers, to a wall or a desk in order to prevent it from being physically removed
- **Server** – A computer that remains on and connected to the Internet in order to provide some service, such as hosting a webpage or sending and receiving email, to other computers
- **SIM card** – A small, removable card that can be inserted into a mobile phone in order to provide service with a particular mobile phone company. SIM cards can also store phone numbers and text messages.
- **Skype** – A freeware Voice over IP (VoIP) tool that allows you to speak with other Skype users for free and to call telephones for a fee. Its developers say that conversations between Skype users are encrypted, end-to-end.
- **Source code** – The underlying code, written by computer programmers, that allows software to be created. The source code for a given tool will reveal how it works and whether it may be insecure or malicious.
- **Spear phishing** – The act of tailoring a fake website or email in order to make it appear authentic to a specific individual or a small group.
- **Spybot** – A freeware anti-malware tool that scans for, removes and helps protect your computer from spyware
- **Steganography** – Any method of disguising sensitive information so that it appears to be something else, in order to avoid drawing unwanted attention to it
- **Swap file** – A file on your computer to which information, some of which may be sensitive, is occasionally saved in order to improve performance
- **Thunderbird** – A FOSS email program with a number of security features, including support for the Enigmail encryption add-on
- **Tor** – An anonymity tool that allows you to bypass Internet censorship and hide the websites and Internet services you visit from anyone who may be monitoring your Internet connection, while also disguising your own location from those websites
- **TrueCrypt** – A FOSS file encryption tool that allows you to store sensitive information securely
- **Undelete Plus** – A freeware tool that can sometimes restore information that you may have deleted accidentally

Digital security links

I. Keep control of your PC

The Basics

- secunia.com/products/consumer/psi/download_psi/
- isc.sans.edu/
- isc.sans.edu/survivaltime.html
- security.ngoinabox.org/en/comodofirewall_main
- alternativeto.net/
- www.osalt.com/
- housecall.trendmicro.com/
- www.bitdefender.com/scanner/online/free.html
- www.microsoft.com/security/scanner/en-us/default.aspx

Some Advanced Techniques

- go.microsoft.com/?linkid=9741395
- go.microsoft.com/?linkid=9743275
- www.grc.com/x/ne.dll?bh0bkyd2
- www.microsoft.com/windows/virtual-pc/default.aspx
- www.virtualbox.org/
- en.wikipedia.org/wiki/Virtual_machines
- windows.microsoft.com/en-US/windows7/products/features/backup-and-restore
- www.todo-backup.com/
- security.ngoinabox.org/en/chapter-1
- security.ngoinabox.org/en/avast_main
- security.ngoinabox.org/en/spybot_main
- security.ngoinabox.org/en/comodofirewall_main
- survival.tacticaltech.org/computer
- www.google.com/goodtoknow/online-safety/phishing/
- www.google.com/goodtoknow/online-safety/malware/

Basic Protection Checklist

- support.microsoft.com/kb/306525
- http://support.microsoft.com/kb/306525
- security.ngoinabox.org/en/comodofirewall_main

II. Protecting Your Data

The Basics

- www.splashdata.com/press/PR111121.htm
- www.microsoft.com/en-gb/security/pc-security/password-checker.aspx
- security.ngoinabox.org/en/chapter-3
- keepass.info/download.html
- security.ngoinabox.org/en/using_keepass
- www.truecrypt.org/download
- www.truecrypt.org/docs/?s=tutorial
- windows.microsoft.com/en-US/windows-vista/File-sharing-essentials
- securityinabox.org/en/truecrypt_main
- windows.microsoft.com/en-US/windows7/products/features/backup-and-restore
- www.cobiansoft.com/index.htm
- security.ngoinabox.org/en/cobian_howtobackup

Some Advanced Techniques

- www.truecrypt.org/docs/?s=tutorial
- security.ngoinabox.org/en/truecrypt_main
- www.todo-backup.com/download/
- security.ngoinabox.org/en/chapter-3
- security.ngoinabox.org/en/keepass_main
- security.ngoinabox.org/en/chapter-4
- security.ngoinabox.org/en/truecrypt_main
- security.ngoinabox.org/en/cobian_main

III. Safer Email

The Basics

- windows.microsoft.com/en-us/hotmail/security?T1=t2
- support.mozillamessaging.com/en-US/kb/manual-account-configuration?s=configure+ssl&as=s
- www.ehow.com/how_8223091_turn-off-images-gmail.html
- office.microsoft.com/en-us/outlook-help/block-or-unblock-automatic-picture-downloads-in-email-messages-HP010355038.aspx
- support.google.com/accounts/bin/answer.py?hl=en&answer=180744
- www.microsoft.com/security/scanner/en-us/default.aspx
- www.comodo.com/business-security/network-protection/cleaning_essentials.php?track=2745&key5sk1=87df603f01aaae03acc1abf058bb1bac233a524e&key5sk2=2128&key5sk3=1334043298000&key5sk10=2005&key5sk11=1334043298000&key5sk12=-2745&key5sk13=1334043308000&key6sk1=&key6sk2=CH1801025162&key6sk3=7&key6sk4=en-us&key6sk5=TH&key6sk6=0&key6sk7=https%253A%252F%252Fwww.comodo.com%252F&key6sk8=112202&key6sk9=19201080&key6sk10=true&key6sk11=298cde2eecbc5eb69d3ae735aa2be8f85261fba7&key7sk1=72&key1sk1=dt&key1sk2=https%253A%252F%252Fwww.comodo.com%252F

IV. Safer Surfing

The Basics

- addons.mozilla.org/EN-US/firefox/addon/noscript/?src=cb-dl-mostpopular
- www.eff.org/https-everywhere
- addons.mozilla.org/EN-US/firefox/addon/https-finder/?src=ss
- addons.mozilla.org/EN-US/firefox/addon/betterprivacy/?src=search
- addons.mozilla.org/EN-US/firefox/addon/wot-safe-browsing-tool/?src=search
- addons.mozilla.org/EN-US/firefox/addon/perspectives/?src=search
- addons.mozilla.org/en-US/firefox/extensions/privacy-security/
- www.eff.org/https-everywhere
- chrome.google.com/webstore/detail/lnppfgdnjafeikakadfopejdpglpiahn?utm_source=chrome-ntp-icon
- chrome.google.com/webstore/detail/bhmmomiinigofkjcapegjjndpbikblnp?utm_source=chrome-ntp-iconwe.riseup.net/riseuphelp+en/openvpn-windows
- hotspotshield.com/
- www.metageek.net/products/inssider/
- www.microsoft.com/security/scanner/en-us/default.aspx
- www.comodo.com/business-security/network-protection/cleaning_essentials.php?key5sk1=5ed0a3d8f28d25396377d3d33ba6468b64cea749&key5sk2=2128&key5sk3=1338810504000&key5sk4=2720&key5sk5=1338810511000&key5sk6=2720&key5sk7=1338810532000&key6sk1=&key6sk2=C
- www.mobileactive.org/howtos/user-guide-to-orbot

Some Advanced Techniques

- 208.69.38.205/
- developers.google.com/speed/public-dns/docs/using
- onorobot.org/en/episode_4
- security.ngoinabox.org/en/chapter-8
- www.howtobypassinternetcensorship.org/
- www.freedomhouse.org/report/special-reports/leaping-over-firewall-review-censorship-circumvention-tools
- en.rsf.org/spip.php?page=article&id_article=33844
- en.rsf.org/beset-by-online-surveillance-and-13-03-2012,42061.html
- www.google.com/goodtoknow/online-safety/safe-networks/
- www.eff.org/wp/blog-safely
- www.eff.org/https-everywhere
- en.cship.org/wiki/Main_Page addons.mozilla.org/en-US/firefox/addon/noscript/?src=ss
- addons.mozilla.org/en-US/firefox/addon/wot-safe-browsing-tool/?src=search
- addons.mozilla.org/en-US/firefox/addon/perspectives/?src=search
- addons.mozilla.org/en-US/firefox/addon/https-finder/?src=search
- advocacy.globalvoicesonline.org/projects/guide/
- www.mobileactive.org/howtos/mobile-anonymity
- www.mobileactive.org/howtos/user-guide-to-orbot

V. Safer Wi-Fi

The Basics

- www.routerpasswords.com/
- security.ngoinabox.org/en/chapter-3
- security.ngoinabox.org/en/chapter-3

Some Advanced Techniques

- www.wikihow.com/Find-the-MAC-Address-of-Your-Computer

VI. Safer Chat and Voice Communication

The Basics

- www.pidgin.im/download/windows/
- www.cypherpunks.ca/otr/index.php#downloads
- security.ngoinabox.org/en/using_pidgin
- portableapps.com/apps/internet/pidgin_portable
- sourceforge.net/projects/portableapps/files/Pidgin-OTR%20Portable/Pidgin-OTR%20Portable%203.2%20Rev%202/
- security.ngoinabox.org/en/portable_security

Advanced Techniques

- trac.torproject.org/projects/tor/wiki/doc/TorifyHOWTO/InstantMessaging

More Resources

- security.ngoinabox.org/en/chapter-7
- security.ngoinabox.org/en/pidgin_main
- survival.tacticaltech.org/computer
- survival.tacticaltech.org/mobile
- security.ngoinabox.org/en/portable_security
- www.eff.org/https-everywhere
- www.mobileactive.org/howtos/off-the-record-messaging
- blogs.skype.com/security/

VII. Reaching Blocked Websites

The Basics

- www.howtobypassinternetcensorship.org/
- tails.boum.org/
- openvpn.net/index.php/open-source/overview.html
- www.torproject.org/download/download.html.en
- support.google.com/news/bin/answerpy?hl=en&answer=1146405
- support.google.com/reader/bin/answerpy?hl=en&answer=113517
- www.icurrent.com/about
- www.torproject.org/projects/torbrowser.html.en

- tails.boum.org/
- sourceforge.net/projects/ovpnp/files/
- security.ngoinabox.org/en/portable_security

Advanced Techniques

- www.howtobypassinternetcensorship.org/
- www.howtobypassinternetcensorship.org/files/bypass-internet-censorship-quickstart.pdf
- flossmanuals.net/bypassing-censorship/ch010_simple-tricks/
- www.howtobypassinternetcensorship.org/files/bypassing-censorship.pdf
- security.ngoinabox.org/en/chapter-8
- www.freedomhouse.org/article/leaping-over-firewall
- en.rsf.org/spip.php?page=article&id_article=33844
- www.eff.org/wp/blog-safely
- advocacy.globalvoicesonline.org/2011/06/21/anonymous-blogging-with-wordpress-and-tor-guide-in-spanish/
- en.cship.org/wiki/Main_Page
- www.mobileactive.org/howtos/mobile-anonymity

VIII. Safer Social Networking and Blogging

The Basics

- support.twitter.com/groups/31-twitter-basics/topics/113-online-safety/articles/481955-how-to-enable-https
- security.ngoinabox.org/en/chapter_3_1
- www.torproject.org/projects/torbrowser.html.en
- www.facebook.com/note.php?note_id=10150172618258920&comments
- support.google.com/accounts/bin/answer.py?hl=en&answer=180744
- en.rsf.org/spip.php?page=article&id_article=33844
- www.eff.org/wp/blog-safely
- security.ngoinabox.org/en/chapter-10
- dev.mobileactive.org/howtos/safer-facebook
- mobileactive.org/howtos/safer-twitter

More Resources

- security.ngoinabox.org/en/chapter-10
- security.ngoinabox.org/en/portable_security
- www.facebook.com/safety/tools/

IX. Really Delete Your Data

The Basics

- www.piriform.com/recuva/download/standard
- eraser.heidi.ie/download.php
- security.ngoinabox.org/en/eraser_main
- www.piriform.com/ccleaner/download/standard

- security.ngoinabox.org/en/settingup_ccleaner
- portableapps.com/apps/utilities/eraser_portable
- www.piriform.com/ccleaner/download/portable
- www.piriform.com/recuva/download/portable
- security.ngoinabox.org/en/portable_security

More Resources

- onorobot.org/en/episode_1
- security.ngoinabox.org/en/chapter-5
- security.ngoinabox.org/en/chapter-6
- security.ngoinabox.org/en/recuva_main
- security.ngoinabox.org/en/eraser_portable
- www.mobileactive.org/howtos/mobile-backups-data-deletion-remote-wipe

X. Respecting the Risks of Sharing Data Online

The Basics

- www.dropbox.com/
- drive.google.com/
- portableapps.com/apps/internet/firefox_portable
- www.torproject.org/
- leakdirectory.org/index.php/Leak_Site_Directory

More Resources

- drawingbynumbers.org/what-can-you-do-about-these-risks
- en.rsf.org/spip.php?page=article&id_article=33844
- www.eff.org/wp/blog-safely
- advocacy.globalvoicesonline.org/projects/guide/
- security.ngoinabox.org/en/portable_security

XI. Safer Cellphones

The Basics

- safermobile.org/resource/mobile-security-survival-guide-for-journalists/#mobile-network-awareness-title
- security.ngoinabox.org/en/chapter_9_1
- www.mylookout.com/news-mobile-security/lookout-lost-phones-30-billion
- security.ngoinabox.org/en/chapter-3
- www.truecrypt.org/
- securityinabox.org/en/truecrypt_main
- itunes.apple.com/us/app/wickr-secure-im-multimedia/id528962154?mt=8
- mobileactive.org/mobile-tools/gibberbot
- guardianproject.info/apps/gibber/
- www.mobileactive.org/howtos/user-guide-to-orbot

- dev.mobileactive.org/howtos/safer-facebook
- mobileactive.org/howtos/safer-twitter
- code.google.com/p/droidwall/
- mobileactive.org/howtos/mobile-surveillance-primer
- securityinabox.org/en/chapter_9_2_1

More Resources

- www.mobileactive.org/howtos/user-guide-to-orbot
- mobileactive.org/howtos/safer-facebook
- mobileactive.org/howtos/safer-twitter
- www.mobileactive.org/howtos/mobile-backups-data-deletion-remote-wipe
- securityinabox.org/en/chapter-9

XII. Applying "Safety First" to Other Technologies

The Basics

- mobileactive.org/howtos/safer-photos-how-remove-location-information-mobile-images
- www.irfanview.com/plugins.htm
- smallworldnews.tv/guide/
- guardianproject.info/apps/securecam/
- market.android.com/details?id=org.witness.sscphase1&feature=search_result

Glossary

- creativecommons.org/licenses/by-sa/3.0/
- security.ngoinabox.org

NOTES

NOTES

NOTES

www.speaksafe.internews.org

Internews
Local voices. Global change.