

## Protect Your Personal Information *Cheat Sheet*

The amount of information collected on each of us is growing astronomically every day. What can **you** do to help protect your—as well as your family’s—information?

**What** information do you want to protect? Here are some categories you might want to consider:

Ad/cookie tracking	Identity information	Reputation
Digital identity	Intellectual property	Social media
Electronic devices	Location	Trash
E-mail	Mailbox	Travel
Family	Medical information	Voting
Financial information	Personal safety	Work information

**Where** are the threats to your information? Here are some common threats:

<p><b>Data loss or theft</b></p> <ul style="list-style-type: none"> <li>• Backup media</li> <li>• Mail/trash</li> <li>• Organization w/ your info goes bankrupt</li> <li>• Paper</li> <li>• Website</li> </ul>	<p><b>Types of Malware</b></p> <ul style="list-style-type: none"> <li>• DNS Changer</li> <li>• Drive-by downloads</li> <li>• Keyloggers</li> <li>• Phishing email</li> <li>• Rootkits</li> <li>• Search engine poisoning</li> <li>• Social media malware</li> <li>• Torrents</li> <li>• Spyware, Trojan Horse, Virus, Worms</li> <li>• Zombies/Botnets</li> <li>• Etc.</li> </ul>
<p><b>Device loss or theft</b></p> <ul style="list-style-type: none"> <li>• Computer</li> <li>• DVD/CD</li> <li>• Backup media</li> <li>• USB drives</li> <li>• Portable electronic devices</li> <li>• Laptop , iPad, smart phones, tablets</li> </ul>	
<p><b>Natural or man-made disasters</b></p> <ul style="list-style-type: none"> <li>• Fires</li> <li>• Floods</li> <li>• Tornadoes</li> <li>• Earthquakes</li> </ul>	<p><b>Personal safety</b></p> <ul style="list-style-type: none"> <li>• Craig’s List</li> <li>• Data Leakage</li> <li>• Identity Theft</li> <li>• Social Media</li> </ul>
<p><b>ID theft</b></p>	<p><b>Social engineering / Pretexting</b></p>

**Who** do you trust with your information? Here are some organizations that you probably trust:

Accountant, lawyer, other professionals	Religious & charity organizations
Employers	Schools & Libraries
Financial institutions—banks, credit unions, loans & credit cards, brokerages	Stores
Government agencies	Social sites
Health care—doctor, dentist, hospital	Websites
Insurance companies	And ...?

**Why** do you trust people or organizations?

- Do they have a legitimate need for your information?
- Do they have policies and procedures to tell you what they do with your confidential information?

**When** do you trust people or organizations?

- Do you give confidential information on the phone, in email, texting, or in person?
- Did you initiate the information exchange?
- If you don’t feel comfortable, don’t do it.

**How** do you give people or organizations your confidential information? Think about advantages and disadvantages to giving out your information in person, over the phone, in email or in text messages, on a secure website. If you’re uncomfortable giving out information in a particular situation: don’t do it! Find another way to give the information.

## General Tips

- Don't leave your electronic devices—cell phones, laptops, tablets, iPads, etc.—unattended in public, including hotel rooms
- Don't use easy-to-guess passwords: <http://www.dailymail.co.uk/sciencetech/article-2063203/This-years-easiest-guess-passwords--discovered-hackers-worked-out.html>
- Don't post private information on social websites. Remember you have no expectation of privacy on social websites.
- Data leakage:
  - Be careful about the information you throw in your trash.
  - Collect your mail as soon as possible.
  - Use vacation holds or have a friend collect your mail if you will be gone for more than a couple of days.
  - Do not announce on Facebook or other social media that you are going on vacation.
- Keep your electronic devices out of sight in your vehicle
- Read software and services licenses.
- Use a password or a pin to protect your smart phone.

## Tools – How to do ...

### Antivirus:

- *Smart phone antivirus comparisons:* [http://www.av-comparatives.org/images/docs/avc\\_mob\\_201209\\_en.pdf](http://www.av-comparatives.org/images/docs/avc_mob_201209_en.pdf)
- *Home user antivirus comparisons:* [http://en.wikipedia.org/wiki/List\\_of\\_antivirus\\_software](http://en.wikipedia.org/wiki/List_of_antivirus_software)  
<http://www.av-test.org/en/tests/home-user/mayjun-2012/>
- *Mac free antivirus:* Sophos- <http://www.sophos.com/en-us/products/free-tools/sophos-antivirus-for-mac-home-edition.aspx>
- *Windows free antivirus:* <http://windows.microsoft.com/en-US/windows/products/security-essentials>

**Clean up your computer:** <http://www.microsoft.com/athome/setup/cleansweep.aspx>

### Computer updates:

- *Mac* <http://support.apple.com/kb/HT1338>
- *Windows* <http://support.microsoft.com/kb/306525>

### Operating systems end of support:

- *XP:* <http://www.microsoft.com/en-us/windows/endofsupport.aspx>
- *Mac OS:* <https://security.berkeley.edu/content/what-know-about-mac-os-x-105-end-life-advisory?destination=node/208>

### Patching programs: Secunia

- *Web-based [needs Java]:* [http://secunia.com/vulnerability\\_scanning/online/](http://secunia.com/vulnerability_scanning/online/)

### Browser safety:

- *Firefox*
  - Automatic updates:** <http://support.mozilla.org/en-US/kb/update-firefox-latest-version>
  - Check for outdated browser plugins:** <http://www.mozilla.org/en-US/plugincheck/>
- *Internet Explorer*
  - Automatic updates:** <http://windows.microsoft.com/en-US/windows-vista/Update-Internet-Explorer>
  - Check for outdated browser plugins:** <http://www.mozilla.org/en-US/plugincheck/>
  - Note: IE 9 will not run on Windows XP**
- *Securing browser:* [http://www.cert.org/tech\\_tips/securing\\_browser/](http://www.cert.org/tech_tips/securing_browser/)
- *Child-safe browser:* <http://www.common sense media.org/website-lists/kid-safe-browsers-and-search-sites>

### Devices:

- Turn off web cams when not in use

- Turn off GPS when not in use

**Device Tracking Software:** <http://preyproject.com>

#### **Digital signatures:**

Do not install programs or drivers if you get an error message that the digital signature cannot be verified.

#### **Disaster Recovery/Backups:**

*Cloud Backups:* <https://spideroak.com/>

*Disaster preparation:*

<http://www.yourownhomestore.com/survival-kit-series-week-23-important-documents/>

<http://online.wsj.com/article/SB10001424052702303627104576410234039258092.html#project%3DDOC110702%26articleTabs%3Darticle>

<http://www.ready.gov/basic-disaster-supplies-kit>

#### **Do Not Track:**

**Encrypting files:** <http://www.7-zip.org/> **[Do NOT lose the password!]**

#### **Firewall:**

- *Microsoft:* <http://www.microsoft.com/security/pc-security/firewalls-using.aspx>
- *Configuring the Mac Application Firewall:* <http://support.apple.com/kb/HT1810>

#### **Identity Theft:**

<http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf>

<http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/filing-a-report.html>

#### **Password Management:**

- *Complex passwords:* <http://www.microsoft.com/security/online-privacy/passwords-create.aspx>
- *KeePass:* <http://sourceforge.net/projects/keepass/files/latest/download?source=recommended>
- *Password Safe:* <http://sourceforge.net/projects/passwordsafe/files/passwordsafe/3.29/pwsafe-3.29.exe/download>
- *Password-protect documents:* <http://office.microsoft.com/en-us/help/password-protect-documents-workbooks-and-presentations-HA010148333.aspx>

**Phishing:** to report phishing email, forward the email with the Internet header to

- FTC: [spam@uce.gov](mailto:spam@uce.gov) – and to the organization impersonated in the email.
- IRS phish: [phishing@irs.gov](mailto:phishing@irs.gov)
- The Anti-Phishing Working Group: <mailto:reportphishing@antiphishing.org>

#### **RFID:**

- *Snoop-proof wallet:* [http://www.ehow.com/how\\_2342369\\_make-snoop-proof-wallet.html](http://www.ehow.com/how_2342369_make-snoop-proof-wallet.html)

#### **Safe Web Surfing:**

- Did you type the website name yourself?
- Should it be a secure website? Does it have a lock displayed in the browser address bar or at the bottom of the website?

#### **Secure your smartphone:**

- *Android and iPhone:* <http://www.extremetech.com/computing/116635-how-to-properly-secure-your-iphone-or-android-device>
- *Windows phone:* <http://www.microsoft.com/security/online-privacy/mobile-phone-safety.aspx>

## Secure Wiping: be very careful with these programs, there is no way to recover from secure wiping.

- *Drives:* <http://www.dban.org/>
- *Files:* <http://eraser.heidi.ie/>
- *SSD drives:* <http://nakedsecurity.sophos.com/2011/02/20/ssds-prove-difficult-to-securely-erase/>

## Secure your Internet cable modem/router/Wi-Fi:

- *General tips:* <http://security.getnetwise.org/tips/wifi>
- Use instructions from your provider or Google specific model. Make sure you change any default passwords and put the new password someplace safe.
- *OpenDNS:* <http://www.opendns.com/opendns-ip-addresses>
- *Securing Wi-Fi:* <http://onguardonline.gov/articles/0013-securing-your-wireless-network#understand>
- *Using Hot spots:* <http://onguardonline.gov/articles/0014-tips-using-public-wi-fi-networks>

## SMS [texting] spam

- Cell phone provider should have tools to help you cut down on this.
- Complain to cell phone provider, especially if you get more than a couple a month!
- Report to FCC - <http://www.fcc.gov/complaints>

## Traveling:

- *EFF:* <https://www.eff.org/wp/defending-privacy-us-border-guide-travelers-carrying-digital-devices>
- *Extremetech:* <http://www.extremetech.com/computing/109483-travel-safe-data-security-on-the-road-and-off-it>

## Articles to read

<http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/deter.html>

<http://www.houselogic.com/home-advice/home-security/how-to-prevent-burglaries/>

<http://it.slashdot.org/story/12/03/10/2351259/prof-j-alex-halderman-tells-us-why-internet-based-voting-is-a-bad-idea-video>

## Other resources

- Bureau of Justice statistics: <http://bjs.ojp.usdoj.gov/>
- Electronic Frontier Foundation: <https://www.eff.org/>
- Microsoft Safety & Security Center: <http://www.microsoft.com/security/resources/default.aspx#Free-materials>
- National Cyber Security Alliance: <http://www.staysafeonline.org/>
- Stop – Think – Connect: <http://onguardonline.gov/topics/secure-your-computer>
- The Internet Crime Complaint Center (IC3)- <http://www.ic3.gov/media/IC3-Poster.pdf>
- Urban Legends Reference Pages: <http://snopes.com/>
- US-CERT [Computer Emergency Readiness Team] has a great deal of information:
  - Resources - <http://www.us-cert.gov/home-and-business/>
  - E-mail lists - <https://forms.us-cert.gov/maillists/>
- Virus Bulletin comparative anti-virus list: <http://www.virusbtn.com/vb100/archive/test?recent=1>

Note: Technology is constantly changing, so you must consider whether the information provided is timely and applicable to your situation.