7 Steps To Increase Privacy When Using The Internet

Software manufacturers, utility companies, hotels, law enforcement, banks, government agencies and criminals all stand to gain from you surrendering your privacy.

They are all selling the lie that you must be a drug dealer or a terrorist if you prefer to communicate anonymously.

It's brainwashing. Don't be a sheeple. Good guys value privacy too.

Americans have traditionally valued privacy very highly. Many still do. Many have "voted with their feet" and moved to less densely populated Western states and Alaska.

"The Greatest Generation" and those who lived through the great depression counted privacy among our inalienable, God-given rights. Americans stood united on the issue from the founding fathers right up until "generation x".

It's pretty easy to spot *when* privacy began its cycle of demise.

But *what* changed? *What* initiated the down-hill slide? *Why* was this cherished fundamental of the American dream devalued? *How* did we lose our grip on it?

These questions affect us all. Many factors joined forces to wage war on privacy, and now it's our turn to fight back taking these seven steps to protect our privacy.

1. Implement Strong Physical

Security

Ever heard that possession is nine tenths of the law? All jurisdictions recognize that you have rights regarding your home or place of residence. Make use of them. They are barrier to those who abide by or at least fear the law. For the rest, you need to make sure your property is not a worthwhile target. Don't leave physical deterrents out of the privacy equation.

On the technology side of the equation, you might have decent security and SOP in place. No passwords written down anywhere near the computer.

But if someone gets into the same room with your computer, there are any number of ways to penetrate that security. They could install a keystroke logger that makes a note of your every keystroke. So do due diligence in regards to physical security.

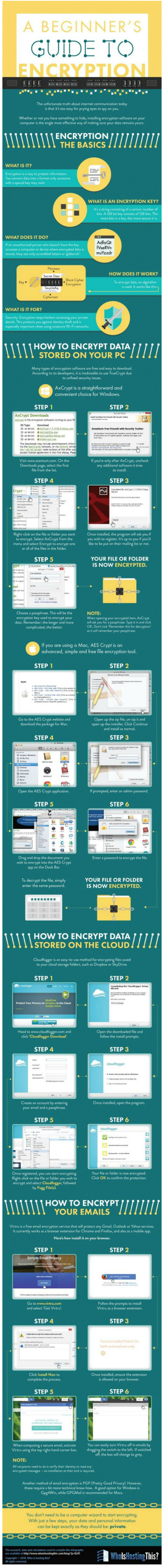
2. Encrypt, Encrypt, Encrypt and Encrypt Some More

Encryption is one of the very best tools in your arsenal. As long as your data is properly encrypted, even if all your other security measures fail, no useful information will come out of the encrypted data … period, end of story.

If you only take one single piece of information away from this steps, make sure it's to create effective data encryption SOP and follow it to the letter.

If you do this one thing, even if your enemies descend upon your home like the US Military on Bin Laden or put crime tape around or bag everything and every property you own, they won't get a shred of useful data.

They will have to rely purely on external, largely circumstantial, sources of evidence.


A BEGINNER'S
GUIDE TO
ENCRYPTION
The unfortunate truth about internet communication today is that it's too easy for prying eyes to spy on you.
Whether or not you have something to hide, installing encryption software on your computer is the single most effective way of making sure your data remains yours.
ENCRYPTION THE BASICS
WHAT IS IT?
Encryption is a way to protect information. You convert data into a format only someone with a special key may read.
WHAT IS AN ENCRYPTION KEY?
It's a string consisting of a certain number of bits. A 128 bit key consists of 128 bits. The more bits in a key, the more secure it is.
WHAT DOES IT DO?
If an unauthorized person who doesn't have the key accesses a computer or device where encrypted data is stored, they see only scrambled letters or 'gibberish'.
AdfaQt fVseRVn muYzzdr
Plaintext
Secret Data
Key
Block Cipher Encryption
TevyUzAq
Ciphertext
HOW DOES IT WORK?
To encrypt data, an algorithm is used. It works like this
WHAT IS IT FOR?
Security. Encryption stops hackers accessing your private details. This protects you against identity theft and is especially important when using unsecure Wi-Fi networks.
HOW TO ENCRYPT DATA STORED ON YOUR PC
Many types of encryption software are free and easy to download. According to its developers, it is inadvisable to use TrueCrypt due to unfixed security issues.
AxCrypt is a straightforward and convenient choice for Windows.
STEP 1
AxCrypt Downloads
Visit www.axantum.com. On the Downloads page, select the first file from the list.
STEP 2
ZoneAlarm Free Firewall with Security Toolbar
If you're only after AxCrypt, uncheck any additional software it tries to install.
STEP 3
Once installed, the program will ask you if you wish to register. It's up to you if you'd like to be put on their mailing list or not.
STEP 4
Right-click on the file or folder you want to encrypt. Select AxCrypt from the menu and select Encrypt to encrypt one or all of the files in the folder.
STEP 5
Choose a passphrase. This will be the encryption key used to encrypt your data. Remember: the longer and more complicated, the better.
YOUR FILE OR FOLDER IS NOW ENCRYPTED.
NOTE:
When opening your encrypted item, AxCrypt will ask you for a passphrase. Type it in and click OK. Don't tick 'Remember this for decryption' as it will remember your passphrase.
If you are using a Mac, AES Crypt is an advanced, simple and free file encryption tool.
STEP 1
Go to the AES Crypt website and download the package for Mac.
STEP 2
Open up the zip file, un-zip it and open up the installer. Click Continue and install as normal.
STEP 3
If prompted, enter an admin password.
STEP 4
Open the AES Crypt application.
STEP 5
Drag and drop the document you wish to encrypt into the AES Crypt app on the Dock Bar.
STEP 6
Enter a password to encrypt the file.
To decrypt the file, simply enter the same password.
YOUR FILE OR FOLDER IS NOW ENCRYPTED.
HOW TO ENCRYPT DATA STORED ON THE CLOUD
Cloudfogger is an easy-to-use method for encrypting files saved to your cloud storage folders, such as Dropbox or SkyDrive.
STEP 1
Protect Your Privacy on SkyDrive Dropbox Google Drive in the Cloud
Head to www.cloudfogger.com and click 'Cloudfogger Download'.
STEP 2
Completing the Cloudfogger Setup Wizard
Open the downloaded file and follow the install prompts.
STEP 3
cloudfogger
Once installed, open the program.
STEP 4
Create an account by entering your email and a passphrase.
STEP 5
Once registered, you can start encrypting. Right-click on the file or folder you wish to encrypt and select Cloudfogger, followed by Fogg File(s).
STEP 6
cloudfogger
Your file or folder is now encrypted. Click OK to confirm the protection.
HOW TO ENCRYPT YOUR EMAILS
Virtru is a free email encryption service that will protect any Gmail, Outlook or Yahoo services. It currently works as a browser extension for Chrome and Firefox, and also as a mobile app.
Here's how install it on your browser.
STEP 1
Simple Email Privacy
Go to www.virtru.com and select 'Get Virtru'.
STEP 2
Follow the prompts to install Virtru as a browser extension.
STEP 3
You've installed Virtru! Go forth and read securely
Once installed, ensure the extension is allowed on your browser.
STEP 4
Click Install Now to complete the process.
STEP 5
ACTIVATE VIRTRU TO COMPOSE SECURE EMAILS
When composing a secure email, activate Virtru using the top right-hand corner box.
STEP 6
You can easily turn Virtru off in emails by dragging the switch to the left. If switched off, the box will change to grey.
NOTE:
All recipients need to do is verify their identity to read any encrypted messages – no installation at their end is required.
Another method of email encryption is PGP (Pretty Good Privacy). However, these require a bit more technical know-how. A good option for Windows is Gpg4Win, while GPGMail is recommended for Macs.
You don't need to be a computer wizard to start encrypting. With just a few steps, your data and personal information can be kept exactly as they should be: private.
The research, data and calculations used to compile this infographic are available at http://www.whoishostingthis.com/blog/?p=8241
Copyright © 2014. Who is hosting this? All rights reserved.
WhoIsHostingThis?

3. Don’t Adopt New Technology Prematurely

Choose not to adopt emergent technology until security bugs have been found and patched and you understand how the new technology will impact your privacy.

There are many reasons not to adopt these new technologies prematurely:

- You pay a premium to be on the “bleeding edge” of technology.
- Why beta-test (troubleshoot) a manufacturer’s new product for them? Waiting until the first round or two of patches or revisions have been made ensures a more robust platform.
- Many new products are highly proprietary when they first hit the market so you will be locked in to the options offered by the manufacturer. Once the other manufacturers have time to respond, you will have far more options to customize the product to your needs, resulting in a superior solution.
- Lastly and most important to this course, it’s much safer to adopt a technology after it has been poured over and reverse-engineered by privacy experts and they have published their findings.

4. Don’t Create New Online Accounts that Hamper Your OPSEC

Delete any that you already have submitted. How many accounts do you have with email services, search engines, banks, investments, utility companies, internet service providers, credit cards, social media, shopping, schools, organizations, backup services, file sharing, software developers, app stores, entertainment, games or other types of websites

online?

And how many of them do you use on a consistent basis?

Remember that every account is a potential OPSEC liability. Learn how to decrease your exposure when you do create accounts.

Some of you may want to get rid of any accounts you created before you learned how to create them and use them without creating undue vulnerability.

5. Configure Your Technology's Privacy Related Settings

Configure content and settings of hardware, software, apps and accounts to reflect the level of privacy you desire and don't choose hardware, software, apps or accounts that will affect your privacy in ways that are unacceptable to you

If you participate in social media using your real name and information, you are volunteering all kinds of information to anyone who's interested.

If your employer or a potential employer, employee or anyone else for that matter looks up information that you voluntarily posted to social media sites that you participate in, that's on you. You put it out there for everyone to see.

Many websites and developers are now at least paying lip service to privacy because folks like us are making a lot of noise about the issue and it's costing them brand equity which translates into money. The result is that privacy settings and privacy statements have come about.

We've argued long and hard for them, so use them. Read the statements and third party security reviews to discern which features and settings of your hardware, software and sites you

use will make a difference.

In many instances, you may need to stop using them and use a competitive product that values your privacy or at least recognizes that the concept still exists. Invest the time to understand and configure your technology's privacy-related settings to protect and limit distribution of your information as opposed to volunteering as much information as possible.

Make use of technology as a tool to effect change on a large scale. Lastly, take into account who each device, software, app or account is created by, their privacy philosophy, where they are physically located, and what jurisdiction it falls under.

The Homeland Security alphabet soup might squeeze American companies left and right or accuse them of being unpatriotic if they don't grant unfettered access to email accounts but that's not as easy to do in another countries.

Some US agencies even infiltrate large companies someone deems vital to national security. They recruit employees to spy for them. This is not exactly top secret knowledge. But that's not as easy to do in other countries, especially in countries that take a dim view of recently exposed US espionage activities.

6. Delete or Destroy

If you ever have to defend your life with a firearm in the US, you will likely have to defend yourself again in court.

Once you've fulfilled your responsibilities of informing the authority and calling for assistance if your attorney was standing to the side and saw the whole thing, he would probably walk over to you and staple your tongue to the roof of your mouth.

He would do it to shut you up because he knows that the burden of proof is on the prosecution and he wouldn't want you saying

anything that might make the prosecution’s job any easier. He would do it even if he was certain you were innocent because he wouldn’t want to give the other side any more resources to work with than they already have.

The same principle applies to privacy, and everything, not just computer files. Crosscut shred paper, redact everything else. If you need to submit receipts for reimbursement, they might need to see your name and the amount, but do they need your credit card billing address or confirmation numbers that might yield more information?

When it comes to information, get rid of anything and everything you don’t need, especially data or computer files of any kind. Give the following criterion a try: if it’s not beautiful, useful or cherished, get rid of it.

Think of it as giving whoever is after your information less to work with. Sanitize everything you can obtain access to as long as you don’t have to break any laws to do so. The more unnecessary copies of data you have laying around, the more complicated the task of managing and securing them will become.

When it’s time to get rid of sensitive information, don’t just delete it or format the drive and throw it in the trash or give it away. Data can be extracted from many storage media even after it has been deleted or the drive has been formatted.

The storage device must be destroyed using data destruction protocols. Destroy the hard drives, SSD’s flash memory, magnetic or optical and any other durable storage medium in such a way that makes the data unrecoverable. Memory technology is constantly in a state of flux.

Different methods are used to destroy a hard drive that stores data on a magnetic medium than a solid state hard drive or an optical disc or a tape drive and so on. It’s a simple matter

to look it up or we can go into more detail in a more in-depth course. The important thing to take away here is to research how to destroy the data on the device before attempting to destroy it.

Do not simply destroy it. If you need to destroy data in a hurry, there are ways to do that. Systems can be created where you can literally "push a button" and walk away, but they usually involve the release of a large amount of energy in the form of heat and light and are noisy.

Video first seen on Snocrash.

7. Remove or Change Sensitive Information from Databases

By law, many businesses must remove your information from their databases if you request it. The largest, most-used non-governmental databases are maintained by large, legitimate businesses. Their internal SOPs require employees to obey the law.

If they didn't, they would expose themselves to huge liabilities, and by law, they must remove you from their database if you request it.

Opt out. You didn't make your digital breadcrumb trail in a day and you're not going to get rid of it in one. Get your identity squared away first and create a new email specifically for this purpose. Choose a secure email provider from those recommended or find one that meets your needs. Don't use that email for anything else but getting removed from email lists.

Many will let you remove yourself without requiring a pound of flesh. Click and you are out. Others will make you email them so they can email you back with a link that will enable you to

remove yourself from the database, that’s where this email will come in handy. They may ask you to send an email requesting removal and will email you the link that will enable you to remove yourself from their database, so it will be more believable if the email resembles your name in some way.

I doubt you’ll come under scrutiny if the name of your email has nothing to do with your name, but it’s a thought. Some companies will demand to see ID. It’s a process, not an event, but it’s worth it.

What you can’t delete or encrypt can often be changed. The vast majority of search techniques search only the most current data available in order to avoid reporting incorrect, information because it’s useless for most purposes. So changing the information, effectively overwrites it in most databases for most purposes.

You need to decide to whom you will give real information and to whom you will give misinformation. In life and as you take steps to improve your privacy, companies will ask you for information. They will turn around and give it or sell it to all of their parent or sibling corporations, affiliates and pretty much anyone with a dollar in their pocket. Direct marketers buy lists of information all the time.

If you conduct a business today, you are asked for sensitive information at every turn. If you refuse to give information, it will create a very awkward moment that gets you noticed at the very least and in many cases they will refuse to do business with you or remove your name form their list if that’s why you’re contacting them.

I strongly caution you against giving false information to the government, commit identity fraud by using another person’s identity or committing credit fraud by lying on a credit application.

You can provide misinformation without breaking any laws, just be mindful of the law. After all, if you’re giving it up, you’re giving up your rights.