Privacy Apps & Tactics

-- .. -.-. .... .- . .-.. -.-. .... -... .-. ---

AnnualCreditReport.com

The only source for your free credit reports. Authorized by Federal law.

Federal law requires each of the three nationwide consumer credit reporting companies - Equifax, Experian and TransUnion - to give you a free credit report every 12 months if you ask for it. Reviewing credit reports helps you catch signs of identity theft early. Take time at least once per year to review your credit report - **https://www.annualcreditreport.com/index.action**

Stopping Unsolicited Mail, Phone Calls, and Email - Tired of having your mailbox crammed with unsolicited mail, including preapproved credit card applications? Fed up with getting telemarketing calls just as you're sitting down to dinner? Fuming that your email inbox is chock-full of unsolicited advertising? The good news is that you can cut down on the number of unsolicited mailings, calls, and emails you receive by learning where to go to "just say no."

The National Do Not Call Registry gives you a choice about whether to receive telemarketing calls at home. Most telemarketers should not call your number once it has been on the registry for 31 days. If they do, you can file a complaint at this Website. You can register your home or mobile phone for free.

Credit Freeze - If you're concerned about identity theft, those reported mega-data breaches, or someone gaining access to your credit report without your permission, you might consider placing a credit freeze on your report.

HTTPS Everywhere is a Firefox, Chrome, and Opera extension that encrypts your communications with many major websites, making your browsing more secure.

https://www.startpage.com/

Encrypted Communication can be used to transmit messages in a confidential way by encrypting them before they are actually sent. It works by catching the contents of a Form's TEXTAREA or other editable elements, you just have to right-click and choose "Encrypt Communication" from the menu.

Mailvelope is a browser extension that enables the exchange of encrypted emails following the OpenPGP encryption standard in webmail services such as Gmail™, Yahoo™ and others.

ChatSecure is a free and open source encrypted chat client for iPhone and Android that supports OTR encryption over XMPP. ChatSecure is available on the Apple App Store and Google Play Store for free.

Cryptocat is an app for having encrypted chat with your friends, right in your browser and mobile phone. Everything is encrypted before it leaves your computer. Even the Cryptocat network itself can't read your messages. Cryptocat is open source, free software, developed by encryption professionals to make privacy accessible to everyone.

Cryptocat does not anonymize you: While your communications are encrypted, your identity can still be traced since Cryptocat does not mask your IP address. For anonymization, we highly recommend using Tor.

Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security. Individuals use Tor to keep websites from tracking them and their family members, or to connect to news sites, instant messaging services, or the like when these are blocked by their local Internet providers. Tor's hidden services let users publish web sites and other services without needing to reveal the location of the site. Individuals also use Tor for socially sensitive communication: chat rooms and web forums for rape and abuse survivors, or people with illnesses.

KeyScrambler

KeyScrambler 3.5 - The moment you begin to type, KeyScrambler begins encrypting your keystrokes in real time at the keyboard driver level. Because KeyScrambler is located in the kernel, deep in the operating system, bypassing KeyScrambler's encryption is difficult. Your keystrokes remain encrypted as they travel through the vulnerable path. If a keylogger happened to be attacking your computer, and if it had escaped your anti-virus program's detection, the keystrokes it captured would be indecipherable and the thieves would get nothing from you. Your keystrokes reach the destination app, the decryption module of KeyScrambler goes to work, and you see exactly the keys you've typed. Here the journey ends with your info intact.

Detekt is a free tool that scans your Windows computer for traces of FinFisher and Hacking Team RCS, commercial surveillance spyware that has been identified to be also used to target and monitor human rights defenders and journalists around the world.

BleachBit quickly frees disk space and tirelessly guards your privacy. Free cache, delete cookies, clear Internet history, shred temporary files, delete logs, and discard junk you didn't know was there. Designed for Linux and Windows systems, it wipes clean a thousand applications including Firefox, Internet Explorer, Adobe Flash, Google Chrome, Opera, Safari,and more. Beyond simply deleting files, BleachBit includes advanced features such as shredding files to prevent recovery, wiping free disk space to hide traces of files deleted by other applications, and vacuuming Firefox to make it faster. Better than free, BleachBit is open source.

CCleaner, developed by Piriform, is a utility program used to clean potentially unwanted files (including temporary internet files, where malicious programs and code tend to reside) and invalid Windows Registry entries from a computer.

Malwarebytes' Anti-Malware (MBAM) is an application for computers running under the Microsoft Windows operating system that finds and removes malware. Made by Malwarebytes Corporation, it was first released in January 2008. It is available in a free version, which scans for and removes malware when started manually, and a paid version, which additionally provides scheduled scans, real-time protection and a flash memory scanner.

Microsoft Security Essentials helps guard against viruses, spyware, and other malicious software. It provides real-time protection for your home or small business PCs. Microsoft Security Essentials is free and we designed it to be simple to install and easy to use. It runs quietly and efficiently in the background so you don't have to worry about interruptions or making updates.

Tails is a live operating system, that you can start on almost any computer from a DVD, USB stick, or SD card. It aims at preserving your privacy and anonymity, and helps you to:

- use the Internet anonymously and circumvent censorship;
- all connections to the Internet are forced to go through the Tor network;
- leave no trace on the computer you are using unless you ask it explicitly;
- use state-of-the-art cryptographic tools to encrypt your files, emails and instant messaging.

GnuPG is a complete and free implementation of the OpenPGP standard. GnuPG allows you to encrypt and sign your data and communication, features a versatile key management system as well as access modules for all kinds of public key directories. GnuPG, also known as GPG, is a command line tool with features for easy integration with other applications. A wealth of frontend applications and libraries are available. Version 2 of GnuPG also provides support for S/MIME and Secure Shell (ssh). **Project Gpg4win** provides a stable Windows version of GnuPG. It is nicely integrated into an installer and features several frontends as well as English and German manuals.

Off-the-Record (OTR) Messaging allows you to have private conversations over instant messaging by providing: *Encryption* - No one else can read your instant messages; *Authentication* - You are assured the correspondent is who you think it is; *Deniability* - The messages you send do not have digital signatures that are checkable by a third party. Anyone can forge messages after a conversation to make them look like they came from you. However, during a conversation, your correspondent is assured the messages he sees are authentic and unmodified; *Perfect forward secrecy* - If you lose control of your private keys, no previous conversation is compromised. Use OTR with **Pidgin** or **Jitsi.**

TrueCrypt is a discontinued source-available freeware utility used for on-the-fly encryption (OTFE). It can create a virtual encrypted disk within a file or encrypt a partition or (under Microsoft Windows except Windows 8 with GPT) the entire storage device (pre-boot authentication). On 28 May 2014, the TrueCrypt website announced that the project was no longer maintained and recommended users to find alternative solutions. TrueCrypt is still a popular, open source encryption program that will meet the security needs of most users. More information about TrueCrypt and access to Version 7.1a is available at: **https://www.grc.com/misc/truecrypt/truecrypt.htm** and **https://truecrypt.ch/**

Other propritaty disk encryption options exist such as **Microsoft BitLocker** and **Symantec Drive Encryption.** If you prefer to stay with free, open source products, consider DiskCryptor for encrypting partitions and AES Crypt for encrypting individual files.

DiskCryptor is an open encryption solution that offers encryption of all disk partitions, including the system partition. DiskCryptor supports AES-256, Twofish and Serpent encryption algorithms. Extra cautions users can also choose to use a combination of cascaded algorithms, which would keep data safe even in case if one of the algorithms would be broken. The encryption key is randomly generated and is stored in an encrypted form, in the first sector of a volume.

AES Crypt is a file encryption software available on several operating systems that uses the industry standard Advanced Encryption Standard (AES) to easily and securely encrypt files.

AxCrypt is the leading open source file encryption software for Windows. It integrates seamlessly with Windows to compress, encrypt, decrypt, store, send and work with individual files. AxCrypt encrypts files that are safely and easily sent to other users via e-mail or any other means. Self-decrypting files are also supported, removing the need to install AxCrypt to decrypt.

Encryption Wizard (EW) is a simple, strong, Java file and folder encryptor for protection of sensitive information. EW comes in two, fully-compatible and interoperable editions, EW-Public and EW-Govt. Anyone can download and use EW-Public. EW is Government invented, owned, and supported software. EW is free to users.

Use a **Master Password in Firefox** to protect stored logins and passwords.

Make the stored password encryption stronger by **configuring Firefox for FIPS 140-2.**

LastPass is a free password management service which seeks to resolve the password fatigue problem by centralising user password management in the cloud. LastPass is standard with a web interface but also includes plugins and apps for many modern web browsers and includes support for bookmarklets. Passwords in LastPass are protected by a master password, encrypted locally, and synchronized to any other browser. LastPass has a form filler that automates password entering and form filling. It also supports password generation, site sharing and site logging.

Two Factor Authentication

Two factor authentication combines something you know, such as a password, with something that you have, such as your cell-phone or a security token. Two factor authentication increases security of your on-line accounts by requiring an additional security step when someone tries to log-in from an unrecognized computer / location. While you can't use two factor authentication everywhere, many popular on-line services allow you to do so. Some places to set up two factor authentication are:

Dropbox

Evernote

Facebook

Google / Gmail

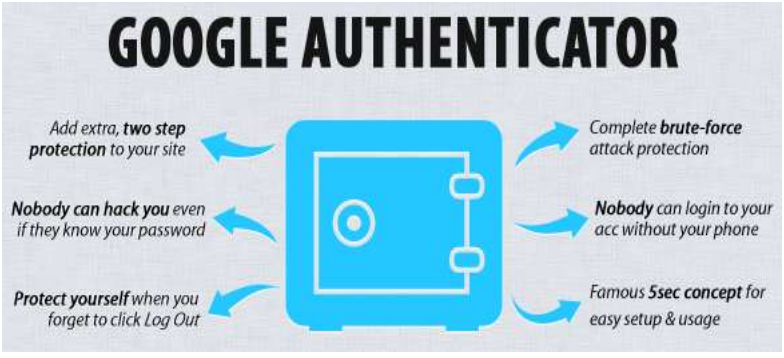
LastPass

LinkedIn

Microsoft Outlook E-mail

Twitter

Yahoo Mail



CYBERSECURITY ONLINE LEARNING

UNITED STATES DEPARTMENT OF DEFENSE
Center for Development of Security Excellence

CDSE Open eLearning Website is the premier destination for accessing security awareness courses for DoD and other U.S. Government and defense industry personnel. These courses are open to the general public.

IASE Information Assurance Support Environment

Cybersecurity Online Training provided by the Defense Information Systems Agency (DISA)

TEEX/NERRTC web-based courses are DHS/FEMA funded and designed as awareness-level training that provides a basic understanding of the course topics. The courses can be taken at any time by individuals at no cost.

… and finally when you want to destroy it all:

Darik's Boot and Nuke
A hard drive disk wipe and data clearing utility

Darik's Boot and Nuke ("DBAN") is a self-contained boot image that securely wipes the hard disks of most computers. DBAN is appropriate for bulk or emergency data destruction.