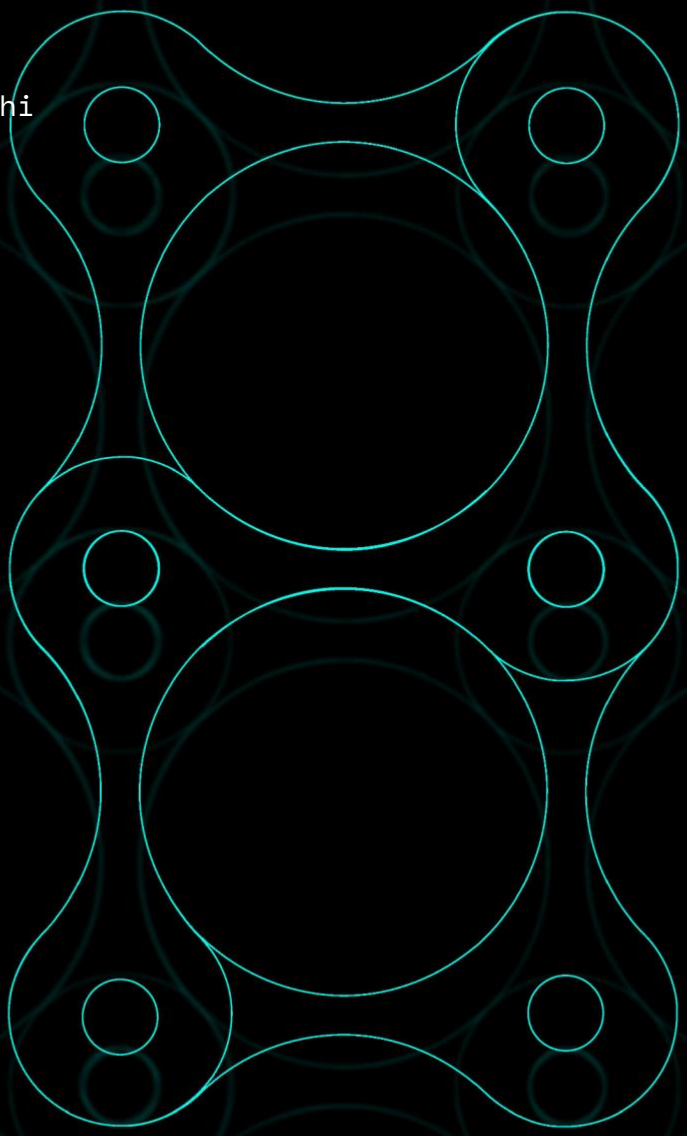
INFORMATION SECURITY MANUAL FOR JOURNALISTS AND CIVIL SOCIETY

By Arianit Dobroshi



INFOSEC
for Balkans

July 2019

TABLE OF CONTENTS

INTRODUCTION

This manual has in mind journalists and other civil society workers of the Southeast European region which currently may not face the most sophisticated information security (infosec) threats. The author believes that it is a worthy tradeoff to sacrifice some information security rigor, if that promotes higher adoption of these practices and tools.

This manual targets audiences with low security practices as well as the general population. As such, is lays out basic information security practices suitable for everyone.

Each section of this manual covers at least two levels of security: the very basic level required for safe computing which should be practiced by everyone, and a higher risk section which every investigative journalist and CSO doing sensitive work in the region should aim for. Nevertheless, some activists and CSOs in the region face even higher levels of threat and should look for other more in-depth resources, some of which are listed in the last section of this manual.

This manual was written in July 2019. Information security threats and their mitigation measures are constantly evolving so this date should be borne in mind when referring to it in the future.

A) WHO IS THIS MANUAL FOR

This manual is aimed at journalists, especially those working in investigative journalism, and civil society activists, especially those dealing with sensitive topics regarding the rule of law. That said, it is a good tool to be used by anyone wanting to upgrade their basic infosec knowledge, especially since it is also available in the languages of the region, which lack resources in this area: Albanian, Bosnian, Macedonian, Montenegrin and Serbian.

The technical level required to implement this work is basic and should be achievable by everyone. Some of the tools do require some sacrifice in usability and practicability from the usual practice.

B) HOW TO READ THIS MANUAL

Each heading of this manual can be read separately based on your immediate information security needs. Nevertheless, it is recommended that you cover all sections of this manual as it is designed as a list of minimum work you should be practicing to protect yourself and your sources. You may come back to it when you have more time and cover all of it. First subheadings cover the very basics that every computer user should already be practicing, though in our observation that is not already the case. he second subheading should provide a security upgrade for most basic users.

Section 2 of the manual covers creating stronger passwords, useful for all platforms. In section 3 we cover your desktop operating system: things you should be doing with your Windows operating system and some help installing Linux Mint, which is a more secure system by default yet easy to use. In section 4 we address browsing securely and in section 5 emailing securely. In section 6 we look at some todo's for mobile system security while at section 7 we address communication security. Finally, section 8 addresses sharing of files, while section 9 gives a list of resources for readers who want to do more.

C) IDENTIFYING YOUR SECURITY NEEDS

Unauthorized access to your data may entail its use, disclosure, disruption, modification, inspection, recording or destruction. However, because digital threats are invisible, complex and often undetectable, they can be underestimated or overlooked.

There are several ways to look at the threats you face and information security needs you have. The most basic threat whole populations face are dragnet threats which every citizen of the region encounters, although more specialized targeted threats may be faced by the target audience of this Manual.

Countries of the region have implemented the EU's Data Retention Directive, which mandates the holding of metadata (data about data) about all telecommunications handled, including lists of all phone calls, IP addresses, text messages etc. sent or received for a period between six to twenty-four months, which may be accessed with a court order. While the communication content itself is not saved, progressing from the legal mandate to wholesale surveillance is not that difficult and the requirement for court order depends on the fragility of the rule of law systems in the region. Even metadata is extremely revealing as it could allow those in possession of it to build social graphs of your life and indirectly identify the content and the sources you engage with, even retrospectively.

With specialized threats, the party conducting surveillance uses specialized and sophisticated tools against the target. The technology for this has been becoming cheaper, and access to it by governments and private parties is becoming easier. For example, it was revealed in 2015 that the North Macedonian government had been tapping the phones of some 20,000 people. There is also evidence that Serbian government was rerouting the internet to certain points, where it could be easily tapped. This was years ago and the situation has likely gotten worse. If you believe you face this kind of threat, then this manual is not enough to protect yourself and you should seek dedicated help.

CREATING STRONGER PASSWORDS

A secure password is random, long enough and combines a list of upper and lower case letters, numbers and other characters (ex. xkvv3.K3?rrz). Nevertheless, it is possible to have secure passwords using combination of words provided it is long enough, unique to the service, random and not associated with you. A combination of random words you could easily remember is a secure enough password (ex. WITHIN-WIRE-GRASS-pluto-save).

A) TWO FACTOR AUTHENTICATION

Whenever available, two factor authentication provides a second means on top of your usual password to secure your web accounts. Second factor of authentication (2FA) may be sent to your phone via a call, SMS, email or may be generated on your Android phone or by a hardware token. You may already be using one for your bank accounts. Second factor adds an extra layer of protection in case your password is compromised.

Enabling second factor authentication depends on your software and you should look under *Settings > Password* or similar to enable it. However, not all services offer it yet.

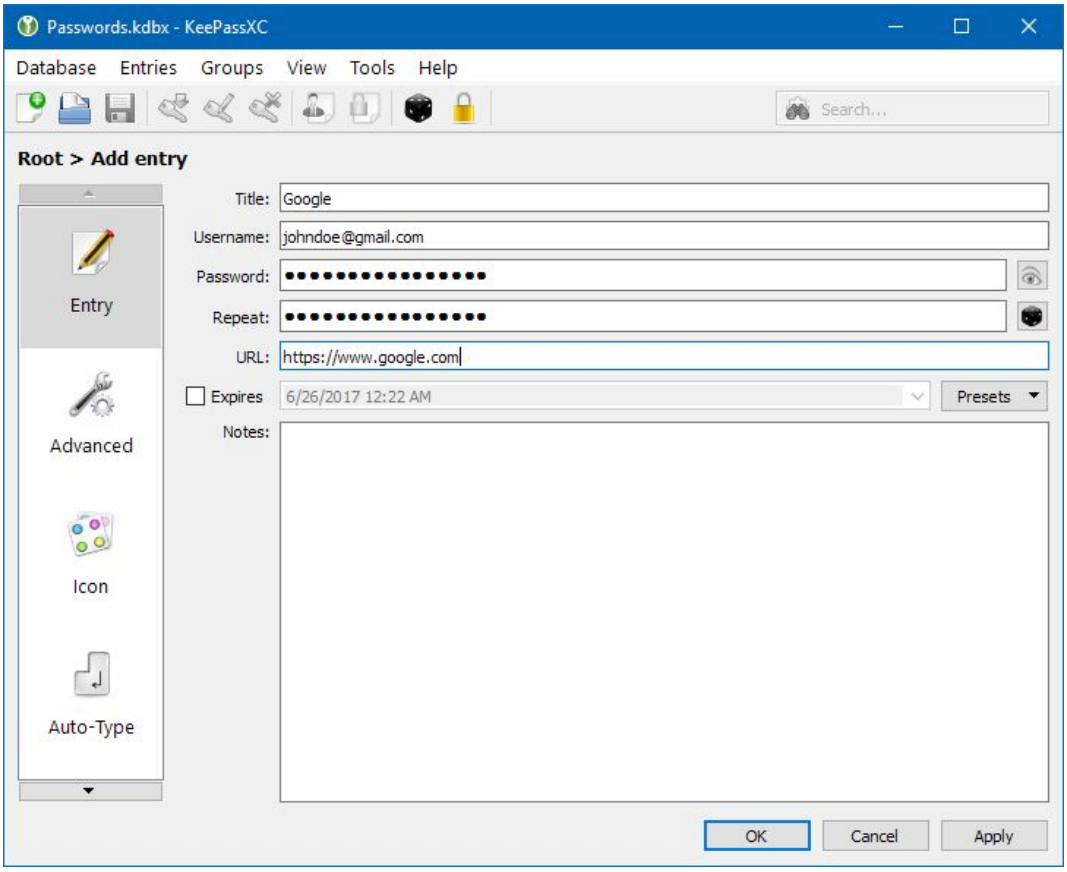
For example, while using Google Services, you may visit **https://myaccount.google.com/signinoptions**, log in with your account, enable it and pick a means to receive your second one time temporary password, normally SMS. Note that if you lose your phone number, you will be locked out of your account. Therefore, you should also set up at least one backup option so that you can sign in even if your other second steps aren't available. Printable one-time passcodes may be the easiest way to allow you to sign in if you lose your number or are traveling.

B) USING SOFTWARE TO CREATE AND MANAGE PASSWORDS

Passwords you use should be unique to each service you use. Memorizing secure passwords soon becomes impossible, necessitating a tool to manage them. To ease creating secure passwords as well as managing them, you may use dedicated software.

A good open source one is KeePassXC(**https://keepassxc.org**) available for Windows macOS and Linux, a password manager that stores usernames and passwords in a local encrypted database, protected by a master password. It also comes with PWGen, a strong random password generator.

Other alternative commercial software are **LastPass** and **1Password**. They store the passwords encrypted online and some features may be available only under the paid version, but they provide better usability and passwords are stored online. Being closed source, it is impossible to audit the security of these two tools independently.



View of KeePassXC screen

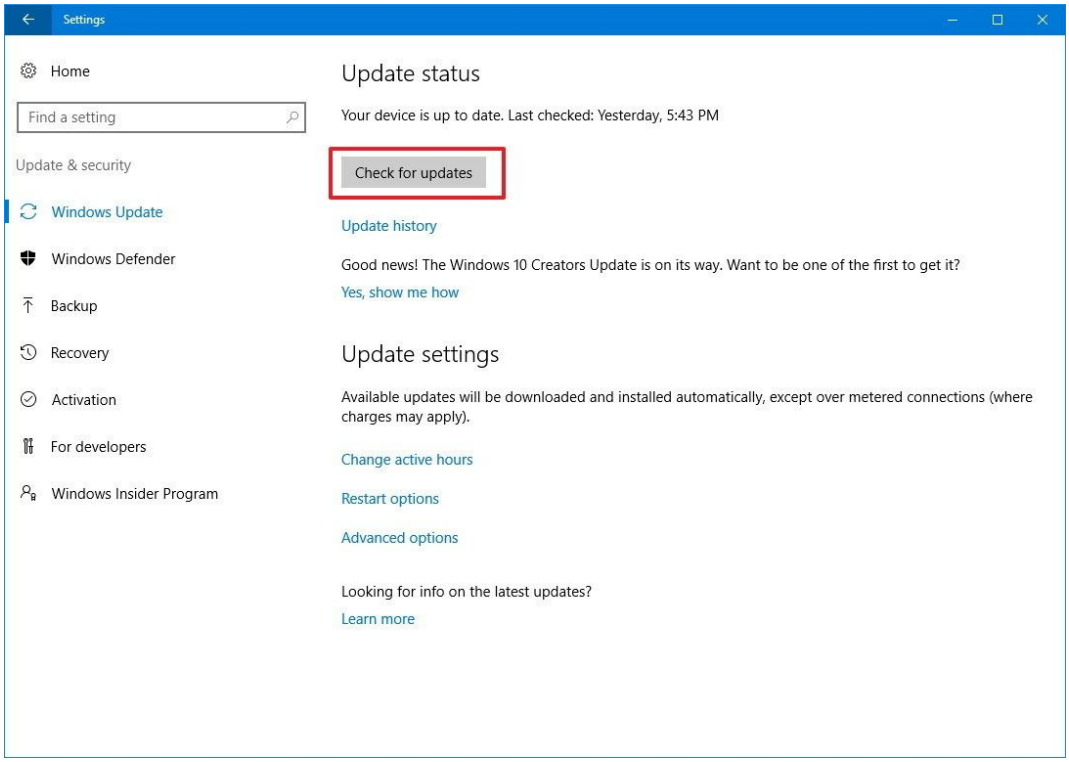
USING A MORE SECURE OPERATING SYSTEM

The desktop operating system is the basis of your secure daily computing. In general, the security of a system ranked from low to high is: Windows 7 or 10 which are most widely used but also least secure, macOS which is more secure by default so is not addressed here, Linux Mint, a Linux system flavor addressed here, and Tails, also Linux based, designed with information security in mind but with usability compromises.

A) KEEPING YOUR WINDOWS UP TO DATE

Keeping your Windows up to date is critical if you work on an internet-connected machine. Too many times, pirated Windows copies are prevented from receiving updates which exposes you to all kinds of malware and other threats. Note that Windows 7 is due to be retired by its publisher Microsoft by the end of 2019 and will therefore not be updated with security patches after this date. You should upgrade to Windows 10 beyond that point.

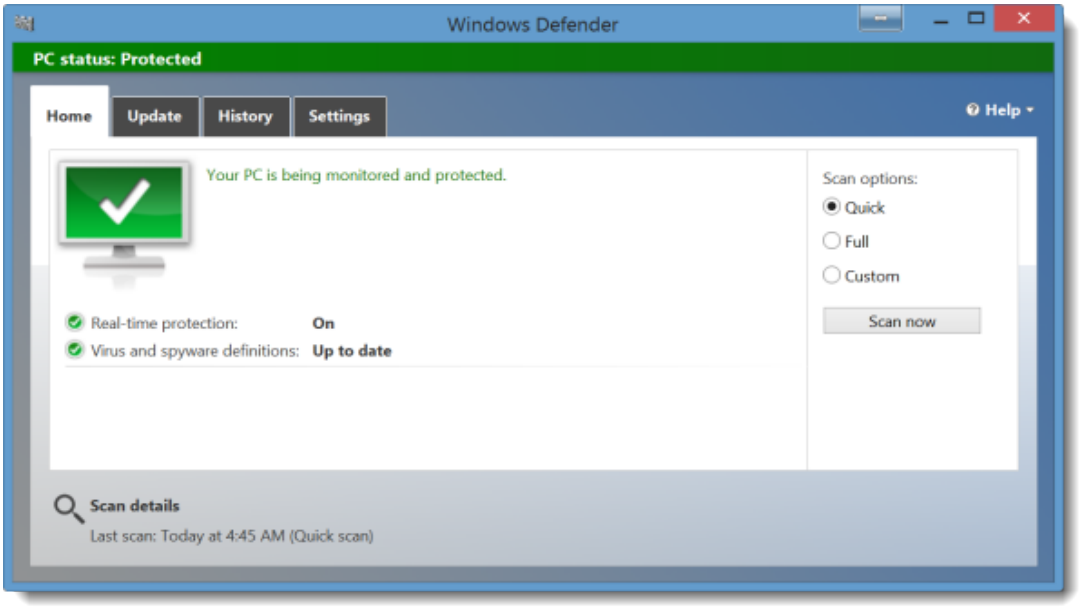
To ensure your Windows is up to date, you should search for "Windows Update" in the Windows search bar, click *Check for updates* and ensure that you receive a screen like the one here which says "No updates are available". Notice that not all updates are security updates and therefore you may ignore those. If a Windows update is impossible to run, then you should seek help to make sure your computer is up to date.



Windows Update status

In addition, you need a software that protects you against viruses and malware. For most cases, the built in Windows Defender is adequate and does not use extra resources on your computer. To run it, uninstall other antivirus software. Go to Windows search bar and type "Windows Defender". Make sure real time protection is on and virus definitions are up to date. If not, you should update them through the Update tab.

If your system has been outdated for a long while, run a full time scan of your system to ensure it is clean, which may take several hours. If you can't resolve any potential findings yourself, you should seek help.

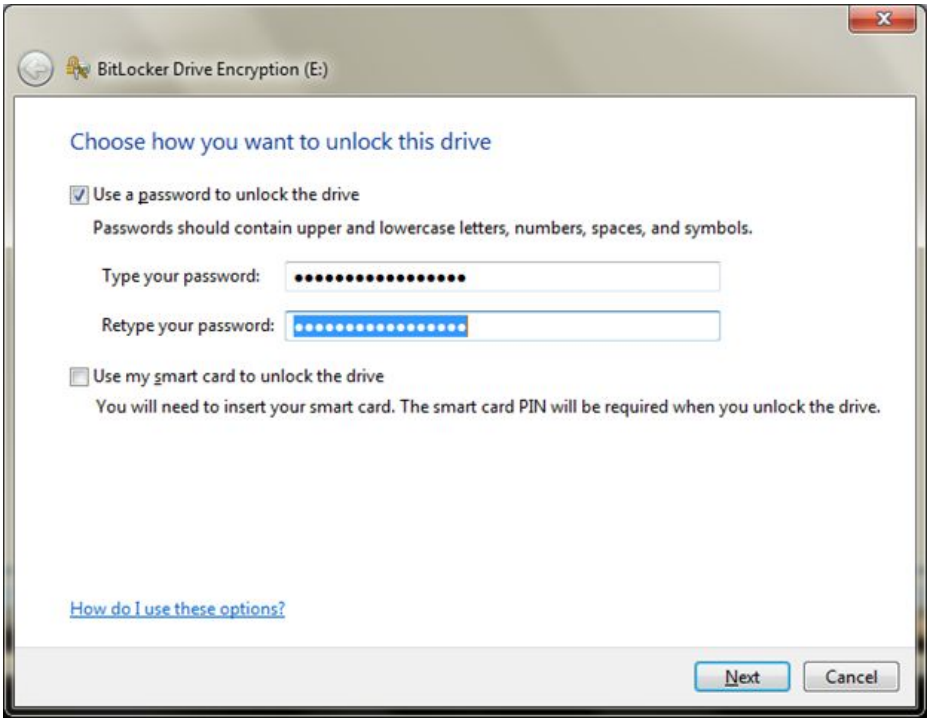


Up to date Windows Defender

B) DISK ENCRYPTION

Data on your computer disk could easily be read by an adversary that has physical access to it if the disk is not encrypted. Most Windows versions up to Windows 7 Pro have no disk encryption installed by default. Windows 7 Ultimate and Windows 10 Pro and Enterprise come with Bit Locker software by default.

BitLocker's full-disk encryption on a system drive requires a computer with a Trusted Platform Module (TPM) built into your PC. This chip generates and stores the encryption keys that BitLocker uses. You can avoid this by using Group Policy to allow use of BitLocker without TPM though you will sacrifice some security.



BitLocker screen

You can encrypt a non-system drive or removable drive without TPM so it's wise to have your data on a separate drive (usually drive 'D'). The easiest way to enable BitLocker for a drive is to open File Explorer and right click the drive, then click on Turn on BitLocker. If you don't see this option on your context menu, then you likely don't have a Pro or Enterprise edition of Windows so you need another alternative.

Warning: BitLocker provides you with a recovery key which you should keep safe by either storing it somewhere safe outside the existing computer or printing it and saving it physically. In case you forget your key or your TPM module is destroyed, this will allow you to access your files again.

If your system drive is encrypted with a password and you have a TPM, you won't notice anything. If you encrypted a non-system or removable drive, Windows prompts you to unlock the drive when you first access it. Type your password to unlock if for use during each reboot.

If you use another operating system such as Linux, disk encryption option is offered during installation. See Linux Mint installation section to see how to enable this.
For all systems, a good independent open source tool respected by security professionals is VeraCrypt (formerly TrueCrypt) accessible here **www.veracrypt.fr**.

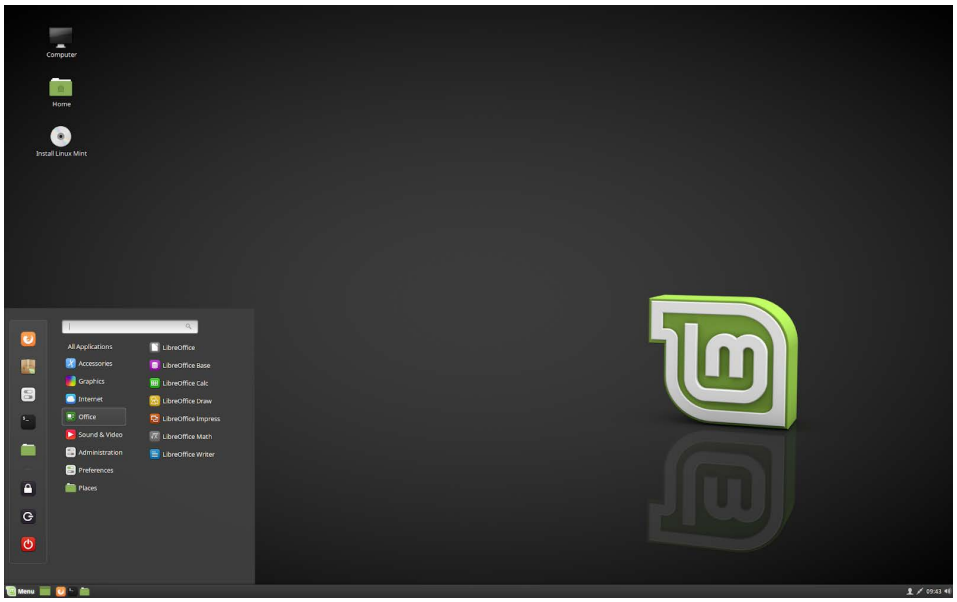
C) LINUX MINT: A MORE SECURE OPERATING SYSTEM

Linux is the free and open source operating system. It is more secure than Windows as it does not face some of Windows' security issues, but will require you to learn a new operating system and at times requires typing in commands to get things done.

There are many "flavors" or iterations of Linux: Ubuntu, Fedora and Linux Mint being the more popular general purpose ones, and Tails being dedicated to those with higher security needs. You should be using whichever version that is most common in your surroundings, so you can seek help if you get stuck. If that is not a feasible option, then go with Linux Mint, which we explain here. It is the most user friendly, has a great support community, is non-commercial, and has a Windows feel for those switching from it.

While Linux has access to a repository of thousands of free and open source software, you may have to learn new applications to get things done, as some software publishers do not publish for Linux. Alternatives to Windows in Linux are: LibreOffice to Microsoft Office, Gimp to Photoshop, Audacity for editing sound etc. Use **http://alternativeto.net** to find alternatives to the software you use in Windows or Mac on Linux.

Next we will show how to install Linux Mint on your computer.



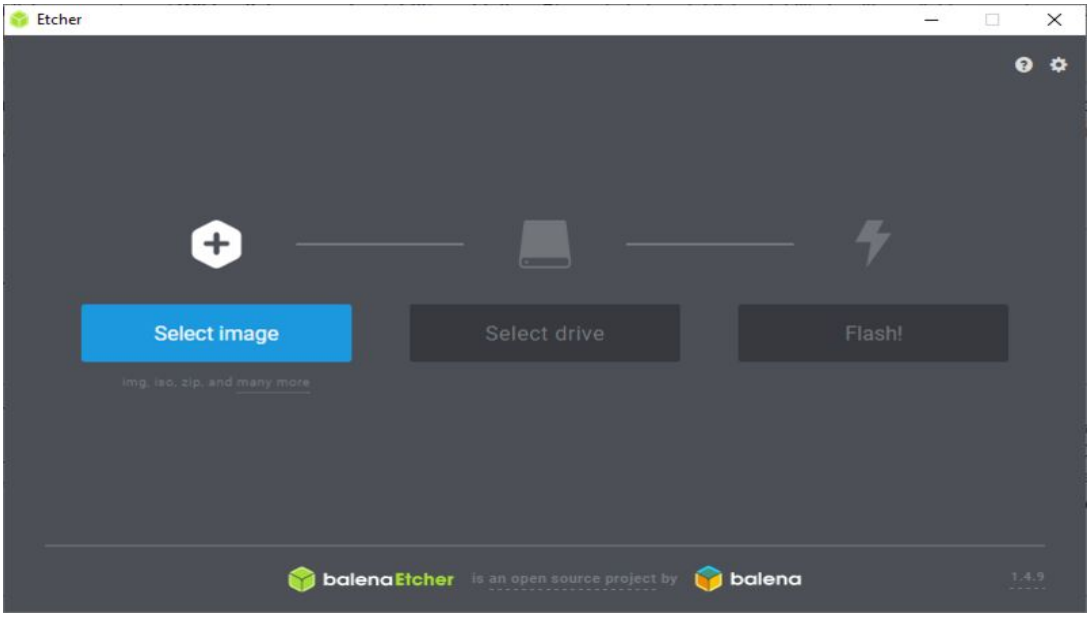
Linux Mint (Cinnamon) desktop

PREPARING THE INSTALLATION USB

1. Backup your data from your Windows system to outside media. It's best to wipe out the Windows installation completely though Windows and Linux can run side by side.
2. Download the Linux Mint Cinnamon ISO here. It may take 30 mins or so depending on your connection: **www.linuxmint.com/download.php**.

BURNING ISO TO USB FLASH DRIVE WITH ETCHER

1. Prepare an empty USB flash drive with at least 2 GB of storage where you will write the ISO file.
2. In Windows or macOS, download Etcher from here **www.etcher.io**, install it and run it.
3. On Etcher click ***Select image*** and select your Linux Mint ISO file.
4. Click ***Select drive*** and select your USB flash drive.
5. Click ***Flash!*** This will burn the ISO to the USB flash drive.



Etcher screen

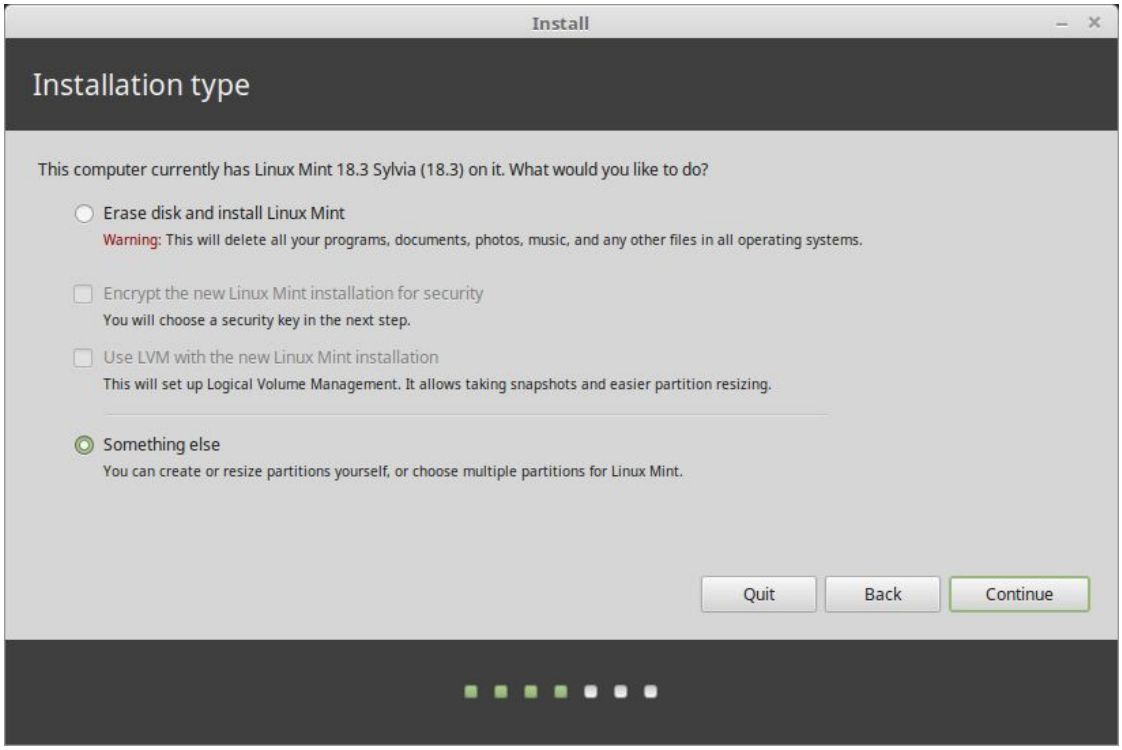
INSTALLING LINUX MINT

1. Boot your PC from the USB drive.
2. When you boot the computer from the USB flash drive, Linux Mint starts a live session. It logs you in automatically and shows you a desktop with the installer on it. You can use this to test how you like Linux Mint.
3. The live session is similar to a normal Linux Mint session once it is permanently installed on the computer, but slower since it's running from the USB drive. Changes you make in the live session are not permanent.

INSTALLING LINUX MINT ON THE COMPUTER

1. To permanently install Linux Mint on your computer, on the Desktop double-click ***Install Linux Mint***
2. Select your language.
3. Connect to the Internet.
4. If you are connected to the Internet, tick the box to install the multimedia codecs.
5. Choose an installation type.
6. If Linux Mint is the only operating system you want to run on this computer and all data can be lost on the hard drive, choose ***Erase disk*** and install Linux Mint.

WARNING



Encrypt the new Linux Mint installation for security refers to full disk encryption. If you are new to Linux use home directory encryption instead (you can select it later during the installation).

7. If another operating system is present on the computer, the installer shows you an option to install Linux Mint alongside it. If you choose this option, the installer automatically resizes your existing operating system, makes room and installs Linux Mint beside it. A boot menu is set up to choose between the two operating systems each time you start your computer.
8. Select your timezone.
9. Select your keyboard layout.
10. Enter your user details. Your username is your account name used to login locally whereas hostname is the name of your computer.
11. To protect your personal data against people who have physical access to your computer, tick Encrypt my home folder.
12. Choose a strong password.
13. Follow the slideshow while Linux Mint is installed on your computer.
14. When the installation is finished, click Restart Now.
15. The computer will then start to shut down and ask you to remove the USB. Upon reboot, your computer should show you a boot menu or start your newly installed Linux Mint operating system.

D) TAILS: AN EVEN MORE SECURE OPERATING SYSTEM

Tails stands for 'The Amnesic Incognito Live System'. It is an open source, Linux-based operating system that protects user's privacy and anonymity. No trace of your computer use is left on the system after shut down, it is privacy- and security- oriented, accessing the internet anonymously by default, thus circumventing any censorship, and comes preinstalled with security-enabled open source tools. It is not addressed in depth here but you should consider it if you feel you are working on very sensitive topics, especially those facing state actors with sophisticated intelligence agencies. See here for more **www.tails.boum.org**.

BROWSING INTERNET MORE SECURELY

Browsing the internet exposes you to numerous risks. This section addresses risks in communication between your computer and the server hosting the web page you are browsing. It starts with a list of add-on's every user should use. Then it explains what VPN is and how to install one. Lastly, for the highest level of risk, it explains Tor and the Tor Browser for safer browsing.

A) ADD-ON PACKAGES FOR YOUR CURRENT BROWSER

You should start by installing a few add-ons or extensions on your current browser either Firefox or Chromium (a version of Chrome without the Google services).

Add-ons

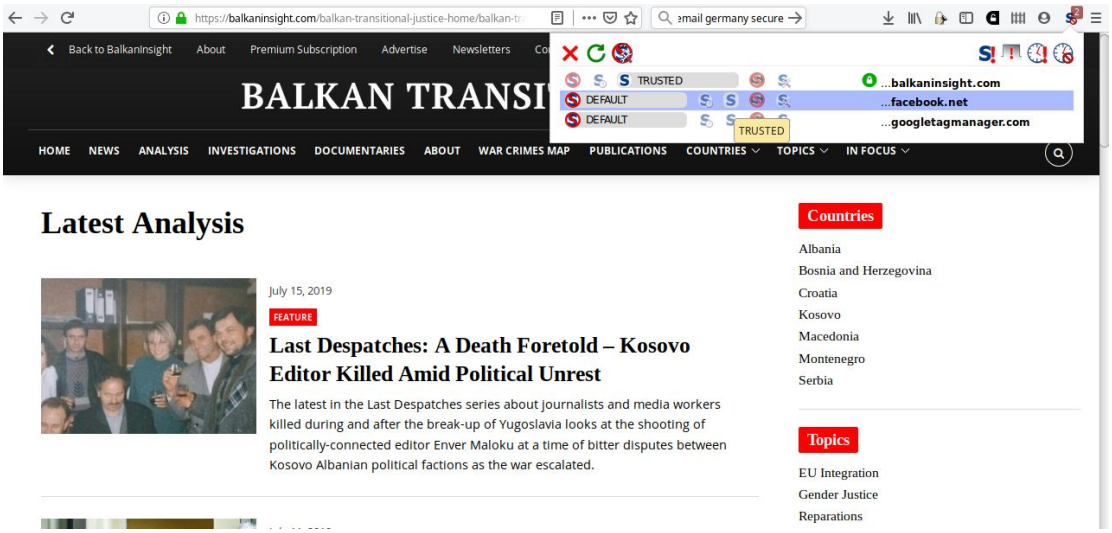
Most popular browsers are certain to make your identity, location and activity available. However, there are some extensions that will help increase privacy and security.

The following extensions available both for Firefox and Chromium are recommended:

HTTPS Everywhere: forces encryption for all connections between your web browser and the web server you are visiting. Note that some websites do not offer such a connection. You can see the status of a particular connection by clicking on the icons to the left of the address bar of your browser.
www.eff.org/https-everywhere

uBlock Origin: an efficient ad and tracker blocker. It is commons for scripts placed in your computer to identify you and track your behavior creating your behavior profile on the web. uBlock Origin blocks all such trackers.
www.github.com/gorhill/uBlock#installation

More advanced: NoScript Security Suite: most of the modern web runs on JavaScript, a scripting language which can be exploited. NoScript allows JavaScript, Flash, Java and other executable content to run only from trusted domains of your choice (e.g. your home-banking site), mitigating remotely exploitable vulnerabilities. If you require more protection, NoScript allows these scripts to run only on sites you trust. That said, it does take some time to build the list of sites you trust by allowing legitimate and necessary scripts while other ones are blocked by default. **www.noscript.net/getit**



View of NoScript Add-on with status of JavaScript on the site (blocking code from Facebook and Google servers)

B) USING VPN

VPN stands for Virtual Private Network. It is a form of tunneling all your information through to another server appearing to others as if it is coming from that other server. This technique masks your IP which can be used to identify your location and possibly you. The tunnel also protects you from prying eyes in your immediate vicinity such as your own ISP or the government in your country. VPN could be offered by your company ensuring for example that your public WiFi connections can't be read. VPN also allows to sidestep any internet filter implemented in your jurisdiction.

However, even with VPN your traffic is still susceptible to monitoring and tracking by the VPN itself, the server of the service you connect to and by other players once it exits the VPN into the public internet.

Selecting a good VPN provider in a friendly jurisdiction with favorable laws is critical. VPN behavior depends on trust and reputation they have built as services and these are not always transparent despite what they may claim, or may suddenly change. Most VPN's are paid by credit card and they can build a profile of your browsing habits which will identify you. Therefore, VPN's are suitable only in certain scenarios to thwart threats in your immediate network.

Two good VPN services are FreedomeVPN based in Finland and ProtonVPN based in Switzerland but you should do your own research to ensure you are getting the best service. They all cost a few euros per month to use but FreedomeVPN offers a basic free tier as well which we will demonstrate here.

Use of ProtonVPN Windows application

ProtonVPN and other service providers publish their own applications mostly for Windows, macOS, Android and iOS which are ready configured therefore don't need any preconfiguration otherwise required. Below is guidance on how to install and connect from a Windows PC. See **www.protonvpn.com/support/** for more help on other operating systems (macOS, Linux, Android and iOS).

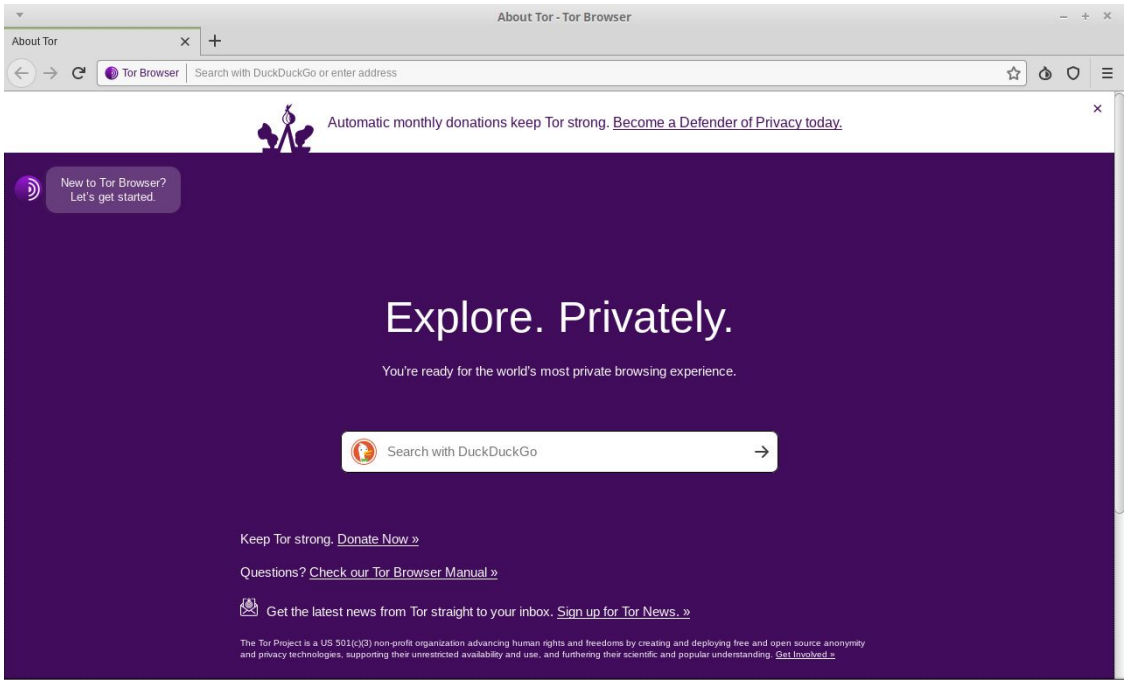
1. Go to **www.account.protonvpn.com/signup** and sign up for the limited plan. If you have a ProtonMail account, you may use that.
2. To download ProtonVPN, go to **www.protonvpn.com/download/** and click **Download for Windows**.
3. When the installation is completed find the shortcut and double-click on it to launch the application. Login screen will appear where you need to enter your ProtonVPN credentials to sign-in. Enter your account credentials created in step 1.
4. When signed-in, you will see the options for quick and easy navigation and connection.
5. Now you can see the country list with each one having a list of VPN servers that you can use by clicking the down arrow. Pick one and click Quick Connect.

ProtonVPN connection screen

6. Note that the free account allows you to access only the free servers in the Netherlands, US and Japan. Pick the one closest to you for better performance, likely Netherlands, or other ones if you need to appear as browsing from those other two countries.
7. You're done.

C) A SAFER BROWSER: TOR BROWSER

Web browsing is subjected to surveillance at various levels. The Tor Onion network is designed to protect against tracking, surveillance, and censorship online. Tor Browser is the secure browser which routes its traffic over the Onion network and has other security enhancements. Each Tor Browser session is unique.



ProtonVPN connection screen

Using Tor Browserg Tor Browser

1. Go to Tor Browser official site to download Tor Browser for your platform **www.torproject.org/download/** There are options for Windows, macOS, Linux and Android. See *Safer mobile browsing* section below for using it on mobile.
2. For Windows, download the .exe file and run it.
3. Click on the Start menu and start Tor Browser.
4. First time you run Tor Browser, you will see the Tor Network Settings window. This offers you the option to Connect directly to the Tor network which should work in Southeast Europe, or to Configure Tor Browser for your connection in case you are using a proxy or Tor connections are blocked by your ISP/country.

Tor browser gives users an option to determine their desired level of safety. In the Tor browser, click on the badge icon (to the right of the address bar) and click 'Advanced Security Options...' to see the options. This option is set to **Standard** by default, which increases usability. To benefit from the higher level of privacy and anonymity that Tor can offer, set the slider to **Safer** or **Safest** level.

EMAILING SECURELY

A) MORE SECURE EMAIL SERVICES

For those who wish to hide the real identities of themselves and/or others they are communicating with, anonymous email accounts should be used, unassociated with any other aspect of your online identity. In other words, they should not be connected with you in any way. Services like Gmail and Microsoft Live request a phone or alternate email address, so these providers are not ideal for anonymous accounts. ProtonMail, Tutanota and Posteo (paid) allow users to create accounts without such identifying information.

B) EMAIL ENCRYPTION ON THE BROWSER WITH MAILVELOPE

Encrypting email using OpenPGP standard is a common practice to ensure that your email messages are not read if intercepted on the way or while at rest on the service provider's servers, as is the case with most commercial email service providers. Email encryption with OpenPGP however is not the most user friendly and if private encryption key is stolen, all messages a party has access to could be read.Furthermore, if the private key is lost, you won't be able to decrypt those messages. Also, encrypted email is not perfect as the addressed and subject line (metadata) can be read if intercepted so have this in mind when using it.

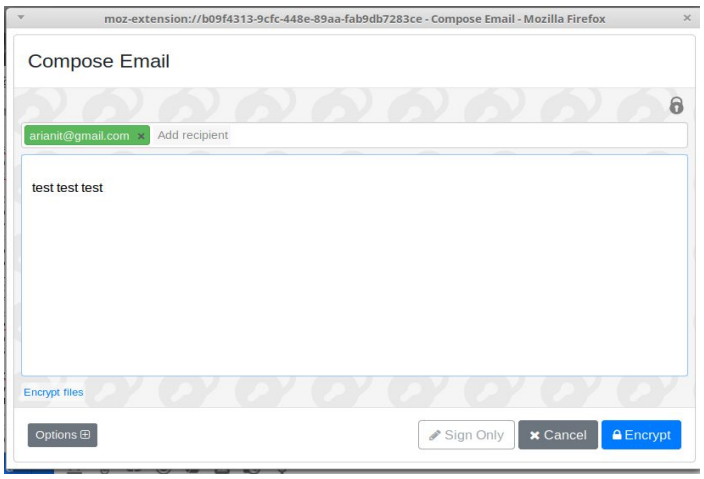
Mailvelope is a free software for end-to-end encryption of email content inside of a web browser (Firefox or Chrome/Chromium) that integrates well with most popular commercial online email services. It can be used to encrypt and sign electronic messages and attachments avoiding a native email client (like Thunderbird) using the OpenPGP standard. It is most useful since it does not force you to switch to a new email client.

Setting up Mailvelope and your PGP key

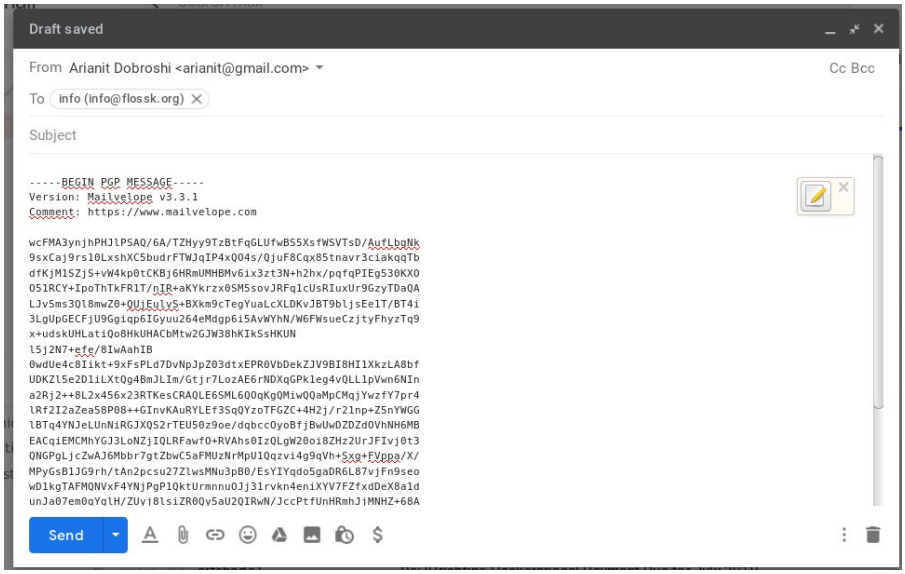
1. Go to Firefox Add-ons and search for Mailvelope.
2. On the toolbar, click the Mailvelope icon. Dashboard screen will open.
3. Click ***Manage keys***. Then ***Generate*** if you don't have an existing key or ***Import*** if you already have one.
4. Enter the fields using the name associated with your email account. Enter a secure password you won't forget otherwise you lose access to the key. Leave other settings default.
5. Click Generate and wait shortly. Your key is now generated and ready to use. A message will be sent to you to be able to upload your public key to the server for others to find. Your public key is what others use to encrypt messages for you. You use your private key to open them.
6. Warning: Your private key should be kept secret. Never share it with anyone.

Sending encrypted emails

1. To encrypt emails to someone, you need first to import the person's public key into Mailvelope. You can receive that directly ex. via email, find it on the person's public website or in one of the Key Servers which hosts keys provided such as those from Ubuntu or MIT.
2. In Mailvelope, go to ***Key management***, paste the text of the public key into the box or click ***Search***. Search by email or name and click on the key's code, which should be something like this E7F3E1D6. Note that while on public servers it is stated that the key belongs to a certain person, this fact can be spoofed, this is why you might want to confirm the key code through some other means with the person that owns the key.
3. Click the key to import it. You are now ready to encrypt email messages and files to that address.
4. If Mailvelope is active, on the message box of your email service (ex. Gmail) you will receive an icon to write your message there instead. That message will be encrypted with the public key of the person you are sending to, provided you have imported their key first.



Mailvelope text box



MailveloView of an encrypted message on Gmail created using Mailvelope

MOBILE OPERATING SYSTEM SECURITY

Most of your computing is now done on mobile, including for sensitive work. Yet mobile security is in a sorry state exposing users to many vulnerabilities. From outdated and unsupported Android systems to apps that ask for too many permissions, you should think hard if you use mobile devices to do sensitive work. Android itself and certain apps, even supposedly secure ones like WhatsApp, will ask you to update your data to the server, which are stored in the clear and could be easily accessible by court warrant or otherwise.

A) BASICS: ANDROID APP SECURITY

While Apple approves mobile apps before they are published on its App Store individually, conducting due diligence for the privacy burden that those apps impose on users, this is not the case with Android apps from Google Play Store.

If you use Android you have probably been asked and given apps access to things like your call history, messages, location, camera, microphone, and more. Before version 6.0, Android asked users to approve permission requests in a package, raising suspicions why a certain app needs access to the microphone if it only dealt with photos.

From version 6.0 on, Android allows users to choose permissions it will give to the app. You should pay attention to what apps you install on your phone. In addition, if you don't plan to use a certain feature of the app, ex. photos tagged with your geolocation, then don't approve those permissions or approve them on a temporary basis only when you need them.

To check permissions already given:

1. Open your device **Settings**
2. Tap **Apps and notifications**. Choose any app, and tap **Permissions** or tap **App permissions** to review permissions based on specific permission.
3. Tap the slider to ***On*** or ***Off*** position. If you are uncertain, disable it. Android will ask you for permission when it needs and you can make the decision based on reasonableness of the request in that situation.

B) BASICS: KEEPING YOUR ANDROID UP TO DATE

Most Android versions are outdated due to the model of software delivery that Google (publisher of Android) uses with its clients (the mobile phone manufacturers). Often times, Google loses control of the update of its software which now is the responsibility of the manufacturer or the carrier who may not have an incentive to support your particular device beyond a limited time. In general, Google branded devices and manufacturer flagship phones have longer support periods. Apple iOS devices are also supported for a longer time. That's why you should always ask for support period with software updates before buying a certain model.

Updating your Android

You can see your device's Android version number and security update level in your Settings. You'll get notifications when updates are available for you if the system is still being updated. You can also check for updates yourself. Note that these instructions may change depending on the Android version. Consult your phone manufacturer's website if you have difficulty following them.

To see which Android version you have

1. Open your device's ***Settings***.
2. Near the bottom, tap ***System > Advanced > System update***. If you don't see ***Advanced***, tap ***About phone***.
3. See your *Android version* and Security patch level under the respective headings.

Get the latest Android updates available for you

When you get an update notification, open it and tap the update action.

If you cleared your notification or your device has been offline:

1. Open your device's ***Settings***.
2. Near the bottom, tap ***System > Advanced > System update***. If you don't see ***Advanced***, tap ***About phone***.
3. You'll see your update status. Follow any steps on the screen.

COMMUNICATING SECURITY

A) BASICS: MESSAGING WITH SIGNAL

Look at these security features while evaluating the instant messaging client you use:

- are messages are encrypted during transit?
- are messages encrypted to the provider if there is one (i.e. not peer-to-peer)?
- are contacts' identities verified?
- is communication secure if keys are stolen?
- is the software code open to independent review?
- is the security design properly documented?
- have there been recent independent code audits?

In this aspect, WhatsApp is better than Viber, and Signal is better than WhatsApp.

Signal fulfills most of the criteria above and is fairly close from the point of usability to the ones you may already be using therefore, it is the recommended one. Signal is available for free on Android, iOS and Desktop (Windows/Mac/Linux), it's open source and has been peer reviewed, covers text, voice and video calls and files, all end-to-end encrypted and while resting on device. That said, it does make some security compromises which we will not address here.

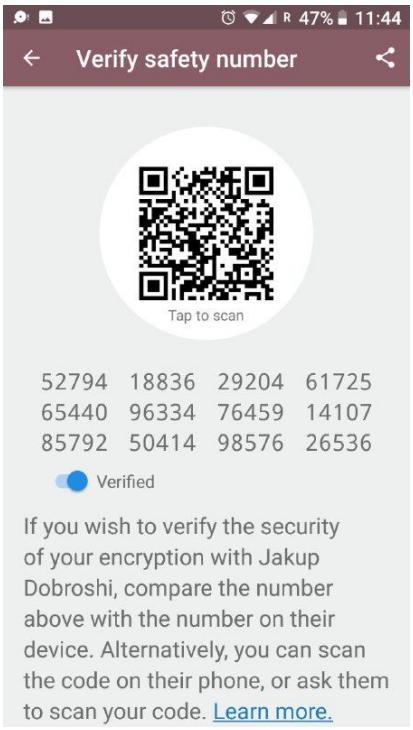
To install Signal on your Android/iOS phone,

1. Confirm that your phone is running Android 4.4/iOS 10.0 or later.
2. Search for *Signal Private Messenger* on Google Play/App Store and install it.
3. Follow the on-screen instructions to complete the registration process similar to other messengers which require you to register your phone number.

Verifying your contacts

On Signal, you are able to verify your contact to ensure that the account you are chatting with really belongs to the person it claims to belong to, and that your secure communication channel has not been tampered with.

1. On Signal, both you and your contact should go to the screen in which you would normally chat with your contact.
2. Tap the three vertical dots icon (upper right corner), then ***Conversation settings > Verify safety number.***
3. Compare the numbers given or hit ***Tap to scan*** the other device with Signal to compare. You may also read it aloud or send it to the party. If they are the same, tap ***Verified***.

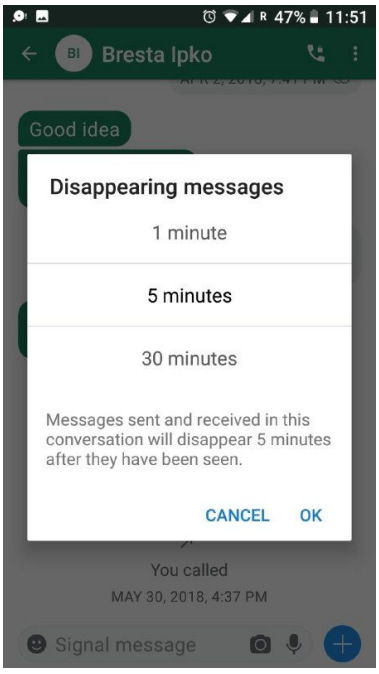


Verification screen on Signal

Disappearing messages

You might want messages to disappear after a set period of time.

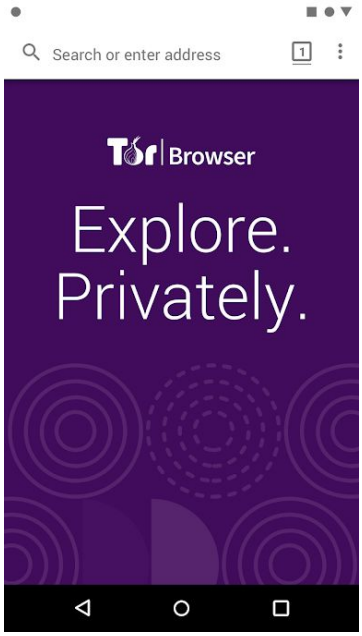
1. On Signal, go to the screen in which you would normally chat with your contact.
2. Tap the three vertical dots icon (upper right corner), then Disappearing messages.
3. In the new screen, select the period. A message will appear in the conversation stating this period.



Disappearing messages screen on Signal set to 5 minutes

B) SAFER MOBILE BROWSING: TOR BROWSER

Tor Browser is also available for Android and iOS. If you use Android, you can download it on Google Play Store by searching for *Tor Browser for Android*. On Apple App Store search for Onion Browser.



Tor Browser on Android

SHARING FILES

Sharing large files securely is a daily struggle. Two ways to send files securely have already been covered, through OpenPGP encrypted email and through instant messaging such as Signal. For larger files, other solutions might be necessary. Below are two other ways to do it. Firefox Send is suitable for low risk scenarios and practical while OnionShare is quite safe, especially if the files have been encrypted first.

A) BASIC: FIREFOX SEND

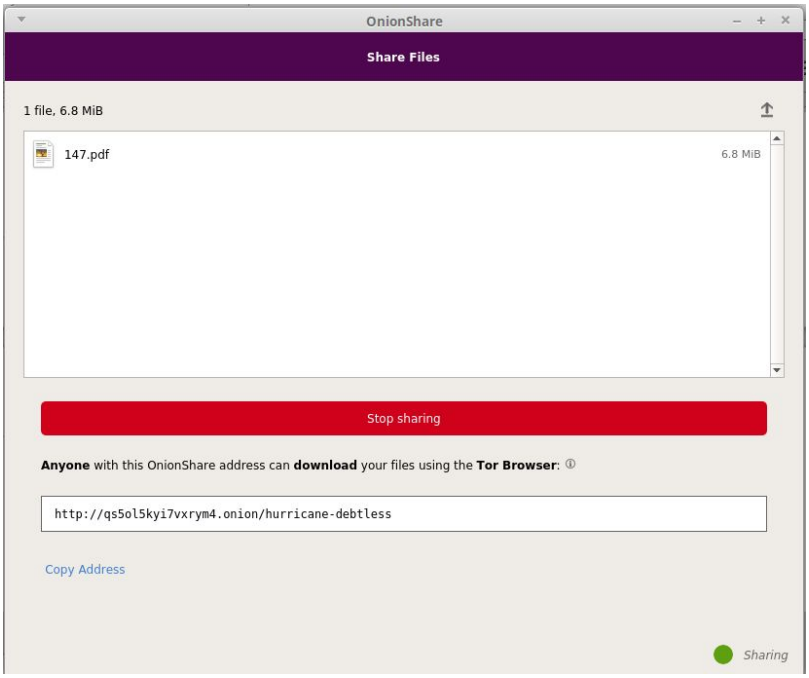
Firefox Send is a more recent solution easy to use. You might want to encrypt the file first using the ***Encrypt a File*** option on Mailvelope (there is a 50 MB limitation) or through other means before uploading the file. To send it, go to **www.send.firefox.com**, select the file to upload and set the options. Note that larger files and more time on server require you to register.

B) SAFER SHARING: ONIONSHARE

OnionShare lets you very securely and anonymously share files of any size. It creates a temporary stealthy web server. An unguessable address is generated and is shared for the recipient to open in the Tor Browser to download the files. While it is very secure, the downside of this tool is that you host the files on your own computer therefore you have to keep it running until it is received by the other parties. The recipient also has to run the Tor Browser in order to receive the files.

To use it:

1. Start by installing OnionShare for your platform from **www.onionshare.org**
2. Once installed, open OnionShare.
3. Add file(s) and click ***Start sharing***. There is no file size limitation. At the end of the process, OnionShare will give you an address such as this one **http://qs5ol5kyi7vxrym4.onion/hurricane-debtles** which you should hand to the recipient through a secure channel. Note that anyone with the address can get access to the file(s) provided your OnionShare with the share is still running.



OnionShare screenshot

WHERE TO GO FROM HERE

If you have outgrown this manual and want more advice or face higher level threats, other good guidance material is freely accessible online, though mostly in the English language and at times outdated.

Security in a Box - Digital security tools and tactics
https://securityinabox.org/

Security in a Box is a project of Tactical Technology Collective and Front Line Defenders. Tactics Guides in this toolkit cover basic principles, including advice on how to use social media and mobile phones more safely. Tool Guides offer step-by-step instructions to help you install, configure and use some essential digital security software and services. The Community Toolkits focus on specific groups of people – sometimes in specific regions – who face significant digital security threats. They include tailored advice on tools and tactics that are relevant to the needs of these particular groups.

Surveillance Self-Defense: Tips, Tools and How-tos for Safer Online Communications
https://ssd.eff.org/

It is a list of guides and lesson plans by Electronic Frontier Foundation.

Information security for journalists, a manual by Centre for Investigative Journalism
https://tcij.org/sites/default/files/u11/InfoSec for Journalists V1.3.pdf

A manual designed to instruct journalists and media organizations on how to practice information security in the digital age, protecting their work, sources, and communications at a variety of risk levels including the highest levels of risk.

Digital Security Helpdesk for Journalists by Reporters Without Borders
https://helpdesk.rsf.org/

Starting in July 2019 RSF will offer free online videos and online consultations on digital security on a regular basis. These seminars can be seen either live or at a later time. Seminars will focus on how to protect social media accounts against hacking, how to sidestep censorship using a VPN, and which smartphone messaging apps are best for journalistic work. More individualized support service will be offered in the future.

ABOUT THE AUTHOR

Arianit Dobroshi is President of the Executive Board at FLOSSK, a non-governmental organization promoting free and open source software in Kosovo. He has trained journalists and members of civil society on privacy tools and lobbied against digital surveillance legislation in Kosovo. He can be reached at **arianit.dobroshi@flossk.org**.

This Manual is done within InfoSec for Balkans project funded by Radio Free Asia – through Open Technology Fund and is implemented by Open Data Kosovo in collaboration with FLOSSK Free Libre Open Source Software Kosova.

Original version was written in English. It is also available in the Albanian, Bosnian, Macedonian, Montenegrin and Serbian languages.


OPEN
TECHNOLOGY
FUND


RFA
Radio Free Asia


ODK
OPEN DATA KOSOVO


Free Libre Open Source Software Kosova