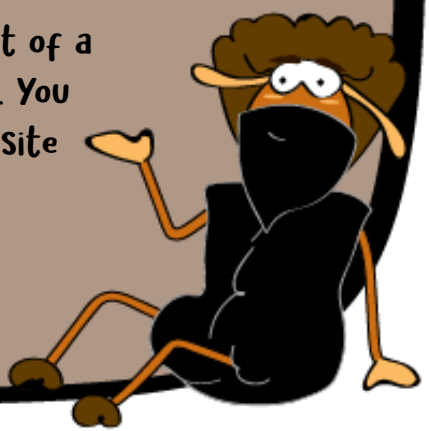
Digital Surveillance Protection and Defense

Online Communications Safety ver-1.0

1. It's always a good idea to start your digital security journey with a risk assessment of your online identity. To check the status of your emails, visit https://haveibeenpwned.com. When you enter your email address on this site it will provide you information if your email has been part of a breach. Breach, meaning that an online service which you used your email to register has been compromised, with the user and password database stolen and possibly posted publicly on the internet. To check if your password has been compromised go to https://haveibeenpwned.com/Passwords.

   If your email account and password has been part of a breach please change your password immediately. You can also register your email accounts on the website

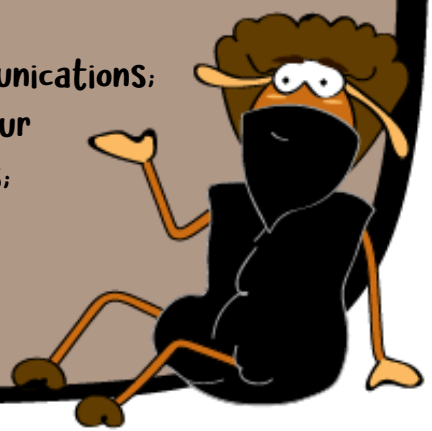


at https://haveibeenpwned.com/NotifyMe to notify you if/when future breaches occur and your account is compromised.

2. Make sure that your online identity is safe by doing identity separation and management. A good first step is to have separate emails for your online services and subscriptions.

   Email accounts are now the preferred way to access your online services and a requirement when subscribing to online services. Having separate emails provide additional privacy and security instead of using only one email for all your online services. (more information on secure email communications below item 4). Below is a recommended online/email identity setup:

   - Separate email account for your work communications;
   - Another account for communications with your families, significant others, and close friends;



- Use and maintain a separate account for your online banking and finance requirements;
- An email for your social media accounts;
- A separate email only for recovering your other email accounts and online services; and
- Use and maintain another account for non-essential communications.

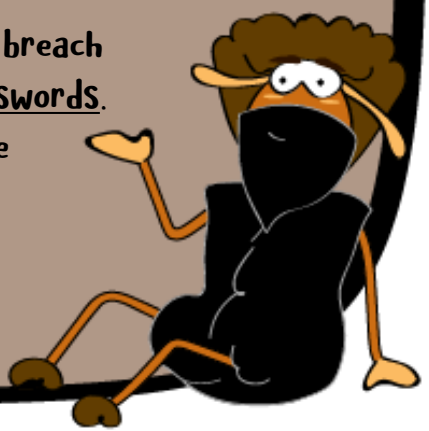
3. Create strong passwords and enable two factor authentication (2fa) to access your online accounts.

   It cannot be stressed enough that the safety of your online account is hinged on the strength of your password. Some tips to create a strong password:

   - Refrain from using personally identifiable information like names, addresses, birthdays, mobile numbers and the like.

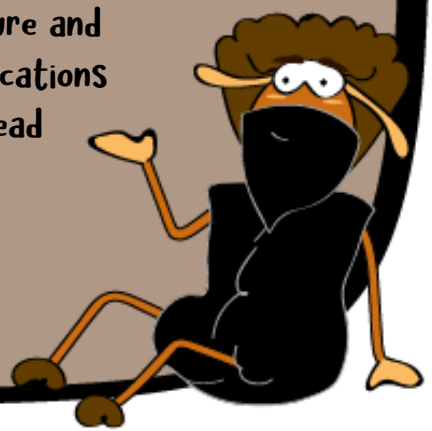
- The password should be a combination of uppercase and lowercase letters, numbers and special characters.
- The longer the password the better. Try to create twice the minimum or more of the required password length of the service or website. For example, Twitter requires a minimum of 6 characters for a password, you should then create a 12 character password or longer.
- Thinking about passwords lends to a gibberish combination of random characters. Think passphrase instead, which could be more meaningful and easy to remember. This can be your favourite song, artist and year you first listened to it, ex. DontStartNowDuaLipa2020!. This can also be a series, ex. CrashLandingOnYou2020!.

To check if your password is already part of a breach please go to: https://haveibeenpwned.com/Passwords.
To check the strength of your password, please visit: https://password.kaspersky.com



To add additional security when accessing your online account, configure two factor authentication (2fa). Two factor authentication is similar to your credit card or bank transactions where a pin code is sent to you via sms for you to enter and verify your transaction. In this case, every time you log onto an online service, the service will require you to enter a pin code for added security.

To check if your online service supports 2fa please refer to this link: https://twofactorauth.org. If supported, instructions on how to setup 2fa for your online service are also available. Please do not use SMS as the 2fa authentication method. SMS is not secure and can be compromised through your telecommunications provider. Use an authenticator application instead for better security.



If you go the route of multiple identities using different passwords and 2fa, it is highly recommended to use a password manager with an authenticator feature.

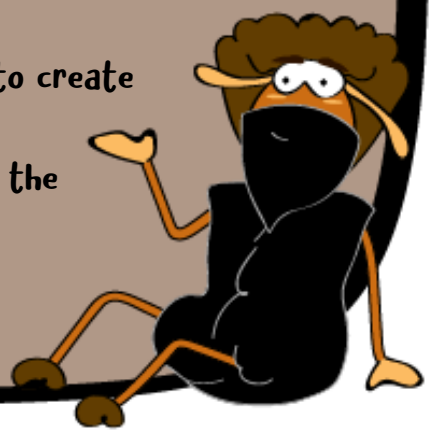
Keepass compatible password managers are applications that can be installed on your computer and mobile devices. They differ in the user interface and additional features but the generated password database files can be used interchangeably across different applications. You can install, for example, KeepassXC on your computer and use the created password database on your Android mobile using KeepassDX. The only downside is you have to manually setup the password database to sync across your devices using a third-party cloud service like DropBox.

- https://keepassxc.org - MacOS and MsWin (Computer) - Free
- https://www.keepassdx.com - Android (Mobile) - Free
- https://keepassium.com - iPhone iOS (Mobile) - Free with paid subscription service for additional features.

You can also opt for a paid cloud-based password manager like Bitwarden. Bitwarden provides a familiar user interface across your computer and mobile devices. The downside is you have to pay for features like 2fa.

- https://bitwarden.com - MacOS and MsWin (Computer), Android and iPhone iOS (Mobile) - Free with paid subscription service for additional features.

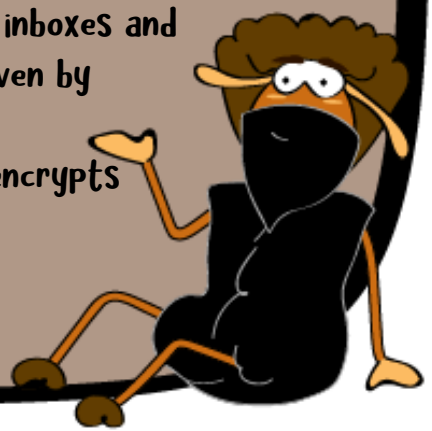
4. For secure email communications, it is advisable to create and maintain email accounts with services that provide end-to-end encryption (e2ee). Below are the recommended services:



- Protonmail
  - Main website https://protonmail.com
  - Free signup https://mail.protonmail.com/create/new?language=en
- Tutanota
  - Main website https://www.tutanota.com
  - Free signup https://mail.tutanota.com/signup

Both email services are accessible via a browser when using a computer (MSWindows and MacOS). Application download is available for mobile devices both for Android and iPhone iOS.

It is important to note that both email services are encrypted on the servers; this means that emails in your inboxes and sent mails are encrypted and cannot be read even by Protonmail and Tutanota. Sending and receiving emails using the same provider automatically encrypts



the contents and attachments. So if you send and receive to and from Protonmail, the emails are encrypted, as with Tutanota to Tutanota. But if you send an email via Protonmail to Tutanota or to GMail and vice versa, the email is not encrypted.

5. For more private and secure communications it is advisable to communicate over data (internet) rather than regular call (GSM/2G) or messaging (SMS). Both GSM/2G and SMS are not private and secure. Mobile providers can tap and monitor both GSM/2G calls and SMS messages. Below are the recommended data messaging applications for both mobile and computers:

   - Signal
     - https://www.signal.org - Main website

   Note: One downside of Signal is that it uses your mobile number to register and this is also your

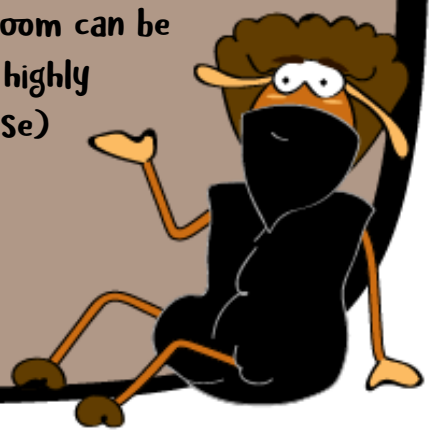
identity on the Signal network. In some cases you might not want to use your personal mobile number as your Signal number. To get around this you can opt to get another SIM and register this as your Signal number. You can keep this SIM in case you need to reinstall Signal.

Another thing worth noting in Signal is the absence of group administration which can be problematic when unauthorised users get into a Signal group. In such cases there is no way to remove the unauthorised user, the only option is for the other users to leave the group and create a new group. With this in mind, Signal is best for one-on-one communications and small groups.

- Wire
  - https://wire.com/en/ - Main website
  - https://app.wire.com/auth/#createaccount - Register a free account

Note: There are several ways to register a Wire account. The recommended method is via a secure email address (please see item 4 above on secure email). Please do not register using your mobile number.

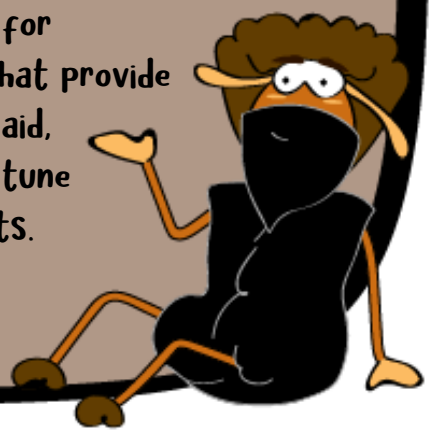
6. For secure video calls and conferences, Signal and Wire provide this feature albeit limited in the number of participants. Signal video and calls are only one-one-one while Wire can have up to 10 participants for voice calls and up to 4 participants for video. If you require more participants for a voice or video call, https://meet.jit.si is the preferred choice. It does not require an account and conference rooms are created automatically by simply visiting the website and clicking on GO. The link that is created can be shared to those participating in the conference. The conference room can be password protected for better security which is highly recommended. Jitsi uses to-server encryption (2Se) to secure your communications from your ISP or



telecommunications company. On your computer JitSi can be accessed via a web browser (please see item 7 below on Secure browsers); on your mobile device, applications are available for both Android and iPhone iOS, https://jitsi.org/#download.

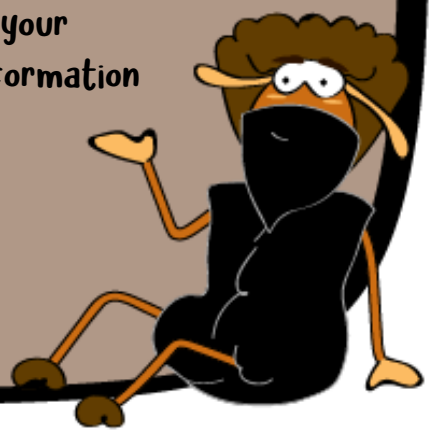
Note: When using https://meet.jit.si it is important to communicate the conference room link and password securely. You can do this by using any one of the Secure emails and messaging apps (please see item 4 and 5 above).

7. A large portion of our online activities are spent viewing information via the browser. Most websites track your identity and movements on the internet for profiling purposes. This is largely for advertising purposes, but the same information can be used for surveillance. Below are the suggested browsers that provide more privacy and security features. That being said, these browsers require further configuration to tune to your specific privacy and security requirements.



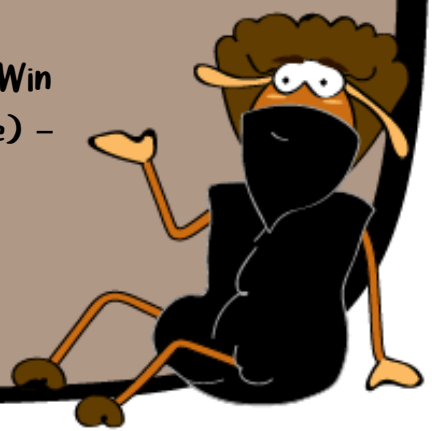
- Firefox
  - https://www.mozilla.org/en-US/firefox/new/ - MacOS and MSWin (Computer)
  - https://www.mozilla.org/en-US/firefox/mobile/ - Android and iPhone iOS (Mobile)
- TOR (The Onion Router)
  - https://www.torproject.org - MacOS and MSWin (Computer), Android
  - https://onionbrowser.com - iPhone iOS (Mobile)

8. To avoid tracking of your online activities it is highly recommended to use a VPN (Virtual Private Network) when accessing the internet. Using a VPN hides the sites that you visit on the internet. This means that your ISP (Internet Service Provider) and/or your telecommunications company will have limited information of your online activity. Remember that ISPs and telecommunications companies hold a lot of our



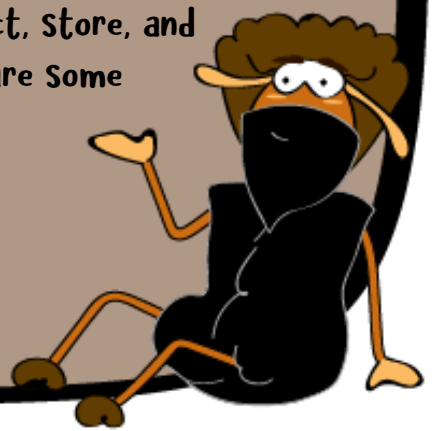
browsing and online history which can be subject to lawful interception as part of surveillance and evidence gathering. Below are the recommended free and paid subscription services:

- RiseUp VPN
  - https://riseup.net/en/vpn – MacOS and MsWin (Computer), Android (Mobile) – Free
- ProtonVPN
  - https://protonvpn.com – MacOS and MsWin (Computer), Android and iPhone iOS (Mobile) – Free for a limited number of different country exit servers. Paid subscription for full access. Note: If you have a free Protonmail account you can use this to access free ProtonVPN service.
- Mullvad
  - https://mullvad.net/en/ – MacOS and MsWin (Computer), Android and iPhone iOS (Mobile) – Paid subscription service



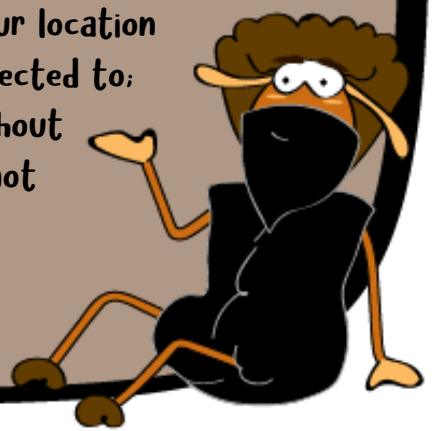
Note: Most VPN services provide multi-device access meaning one subscription or account can be used for multiple devices. ProtonVPN allows for 10 (ten) devices while Mullvad gives you 5 (five). Riseup VPN on the other hand does not require an account, simply install it on your devices and it will connect to a VPN server without account registration.

9. To avoid tracking of your physical location via your mobile device, it is important to manage the GPS (Global Positioning System) feature of your device. The GPS chip on your mobile collects location information which is quite accurate depending on your current environment. The insecurity lies with the applications that you install that can access the data provided by the GPS chip. When applications have access to this location data, they can collect, store, and transmit this data for varying purposes. Below are some measures to prevent this:



- Install only the necessary mobile applications that you need. Uninstall applications that you do not use. Some applications are installed by default and cannot be removed, in such cases you can disable them.
- As a general rule disable location services on your mobile device.
- Only allow applications that require location information to access the location services. (ex. Mapping and transport applications).
- Only allow applications access to location services when you are using the application.

Note: It is important to understand that your mobile device is a tracking device. Your mobile provider knows your location relative to the mobile tower that you are connected to; this is an intrinsic part of this technology: without these tracking mechanisms your provider will not



able to deliver your call and messages. The location information that is collected and maintained by your provider is also the subject of possible surveillance and lawful interception. Please always be mindful of this, more so when attending certain activities.

This resource only provides you a general overview of the different aspects of online communications safety. Most tools and applications presented here require further configuration. The tools are effective only when used properly.