

✓ Money Trail security checklist

This 2-sided security checklist aims to help you identify areas of concerns. This checklist doesn't replace a personal digital security audit. Please tick all that apply. For more information and personal advice, visit <http://security.money-trail.org>

✓ Computer and device security

Decide if the following statements are true about all your devices (computers, laptops, mobile phones).

<input type="checkbox"/>	I use genuine software on my devices. I don't use software that's illegally downloaded.
<input type="checkbox"/>	My devices have recent and up-to-date operating systems (Windows, Mac OS, Linux, Android, iOS).
<input type="checkbox"/>	The software on my devices is up-to-date. I use automatic updates to keep my software up-to-date.
<input type="checkbox"/>	I have a virus scanner on my computer and I keep my virus scanner up-to-date.
<input type="checkbox"/>	I use disk-level encryption to protect the data that's stored on my devices. – Some devices have disk-level encryption built in. We recommend VeraCrypt (https://www.veracrypt.fr).
<input type="checkbox"/>	I use a strong password to login. I'm aware of the risks of fingerprints or facial recognition.
<input type="checkbox"/>	My internet connection has an additional layer of protection, such as a VPN.
<input type="checkbox"/>	I regularly make back-ups of all the important information stored on my devices.

✓ Communications security

Decide if the following statements are true about your communication channels (email, messaging).

<input type="checkbox"/>	I avoid insecure communication channels, such as email and SMS.
<input type="checkbox"/>	I use end-to-end encrypted channels, such as encrypted email and WhatsApp.
<input type="checkbox"/>	For sensitive communication I rely exclusively on tools such as Signal or Wire.
<input type="checkbox"/>	I don't discuss investigations in public communication channels (Facebook, Twitter, LinkedIn).
<input type="checkbox"/>	I don't connect with sensitive contacts on public platforms (Facebook, Twitter, LinkedIn)

✓ Account security

Decide if the following statements are true about all your important accounts (email, cloud, social media).

<input type="checkbox"/>	All my email, cloud and social media accounts are protected by strong and unique passwords.
<input type="checkbox"/>	I use a password manager to create and remember account passwords. – We recommend the free KeePassXC (https://keepassxc.org/) for password management and OTP.
<input type="checkbox"/>	I use second factor authentication (2FA or OTP) for all my important internet accounts. – We recommend the free KeePassXC (https://keepassxc.org/) for password management and OTP with the following apps: Google Authenticator or FreeOTP.

For more information and additional security recommendations, visit the Money Trail security headquarters <https://security.money-trail.org>.

	I keep the amount of personal information on my public profiles to a bare minimum.
	Access to my public profiles on social media is restricted to direct connections.
	I don't store sensitive information in public clouds (Google Docs, Microsoft OneDrive, Dropbox...).
	If I have to use public clouds I encrypt my files before uploading them online. <i>We recommend VeraCrypt (https://www.veracrypt.fr) to encrypt files.</i>

✓ **Data and metadata**

Decide if the following statements are true about all your data carriers (USB drives, mobile devices).

	When I take documents and data with me, I make sure I use strong encryption. <i>– We recommend VeraCrypt (https://www.veracrypt.fr) to encrypt USB drives and external hard drives.</i>
	I'm aware of the risks of metadata that my mobile devices record and share, such as location data. <i>– Mobile phone providers keeps records of your phone's location, and typically store this information for months or years.</i>
	When meeting sensitive contacts I make sure I leave my mobile phone at home or at the office. <i>– To link you to your contact, it can be enough to show that two phones are in the same place at the same time. It is not enough to remove or change your SIM card as your mobile phone also has a personal ID number (IMEI number).</i>

For more information and additional security recommendations, visit the Money Trail security headquarters <https://security.money-trail.org>.