Encryption for Governments

How to Pick Secure Communications Services

December 2021

1 Does the Service Use End-to-End Encryption?

What is an end-to-end encrypted communication? A communication that can only be decrypted by the sender and the receiver. No one else can see the content. Examples of messaging services that offer end-to-end encryption are Signal, WhatsApp, Threema, Telegram and Wickr. Some email providers also offer end-to-end encryption, such as Protonmail and Tutanota.

2 Is End-to-End Encryption Turned on by Default?

People rarely change default settings in apps and services. So, choose encrypted services that apply end-to-end encryption by default. Not all end-to-end encrypted messaging apps have end-to-end encryption turned on by default–you or one of your colleagues might actually send a message that is not protected by end-to-end encryption, and potentially expose confidential or personal data.

3 Does it Use Strong and Up-to-Date Encryption Standards?

For instance, are your websites secured with TLS 1.3? This is the latest version of TLS, used in HTTPS. It is currently the most secure version of the protocol. Earlier versions of TLS may allow vulnerable cryptographic algorithms to be used. TLS 1.3 supports encrypted service name indication (ESNI) which protects against disclosure of the website the user is visiting. Use your browser to check a website's security settings, including the TLS version it is using. You can also check the security features of your own websites through Internet.nl's Test your website tool.

4 Is it Open Source?

A service that is open source has made its code publicly available for others' scrutiny and further testing. This makes security flaws easier to expose, and helps the service to improve constantly, making it more robust against security threats. Both Signal and Threema are open source. WhatsApp's encryption is also based on the Signal protocol, but its code is not open source.

5 Has the Service Been Well-Vetted by Security Researchers?

Regular independent security audits help identify vulnerabilities, software bugs and configuration issues that the service might have missed. Publishing the results of those audits and the action the service has taken to address any concerns helps ensure that the service is actively addressing security issues in a timely fashion.

6 Don't Try to Build Your Own

Correctly implementing encryption, particularly for group conversations, is not easy. You should be wary of trying to build your own service. Also, as apps don't tend to be interoperable, a bespoke app, designed for one organization, is unlikely to be useful for external communications.

Internet Society

7 Does the Service Minimize the Data it Collects?

Read the privacy policy and terms of service carefully before choosing a service. Pay attention to what metadata is exposed and how it will be used by the service. Examine what personal data the service collects from the people who use it and their devices, and what data it pulls in from other sources. Ascertain which country's laws apply to the service provider and its service.

8 Make Sure Backups are Secure

It is often important to keep backups of data, especially for official records. Backups should be stored in an encrypted format, such as on an encrypted device or in encrypted cloud storage. If your organization uses an external cloud storage service for backups, make sure others cannot decrypt the backup. Only your organization should have the keys to do this.

9 Does the Service Support Two-Factor Authentication?

Two-factor authentication provides additional security for your account by requiring another step for login besides using a username and password. An attacker might be able to guess, find or otherwise break your password, but it is harder to break into an account that is also protected by two-factor authentication. Common examples of two-factor authentication are: information you know (e.g., pre-shared answers to security questions), or something you have (e.g., a hardware key such as Yubikey or Google Titan Security Key). Some services might use SMS to send a one-time code. But, as SMS messages are not end-to-end encrypted, an attacker could intercept the code. It is better to use a security key or an authenticator app.

10 Do You Have Clear and Enforceable Guidelines on Using Messaging Services and Record Keeping?

Information that has been shared through end-to-end encrypted services may need to be disclosed in the future. The information might be used in legal proceedings, to fulfill a freedom of information or privacy law request, or because a public access period has started. Government organizations should have clear and enforceable guidelines on the appropriate use of these services, and how they manage electronic records. These policies should include rules on who can access the information, how long information should be retained, and whether to allow the use of "disappearing messages".

Additional Resources:

Internet Society fact sheet – Working from Home

U.S. NSA document – Selecting and Safely Using Collaboration Services for Telework

Internet Society