# Your data and the internet: Security behind the screens

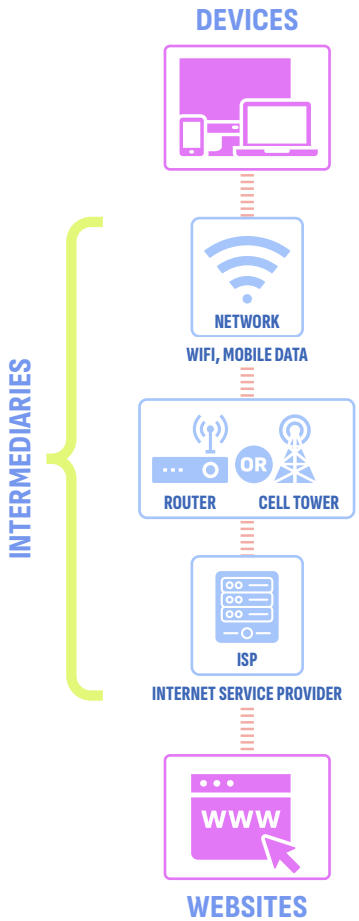
To access a website, we normally open a browser on the device and enter the website's address. This action initiates a series of connections through the device, ultimately delivering the website to our screen.

**See DIAGRAM A for an overview of the connection processes using Wi-Fi or mobile data.**

These processes raise a key question: can intermediaries like Internet Service Providers (ISPs) or router administrators access our information, and if so, what can they see? When considering security, we must therefore ask how our devices, communication channels, and visited websites are protected, and who can access or see information in case of a breach.

Underline denotes glossary word: see page 6.

**A Connecting to a website**




## How can we protect our devices?

Devices contain a wealth of information which may be of interest for any third party who would like to access it physically or via a malware. If someone gains physical or remote access to a device, they can, for example, read and modify files, see all the chats and contacts, and access applications and logged-in accounts.

**To protect the devices from malware**, it is essential to have licensed and updated operational systems and software. It is also crucial to be able to recognize phishing emails and messages claiming to be from trusted sources that actually attempt to harm our devices.

**To protect the devices from unauthorized physical access**, especially from scenarios like seizure or theft, it is crucial to implement security measures such as data encryption or full-disk encryption. Additionally, it is important to protect your devices and data with long, unique, and random passwords that you can securely store in a password manager or retrieve by using recovery options.

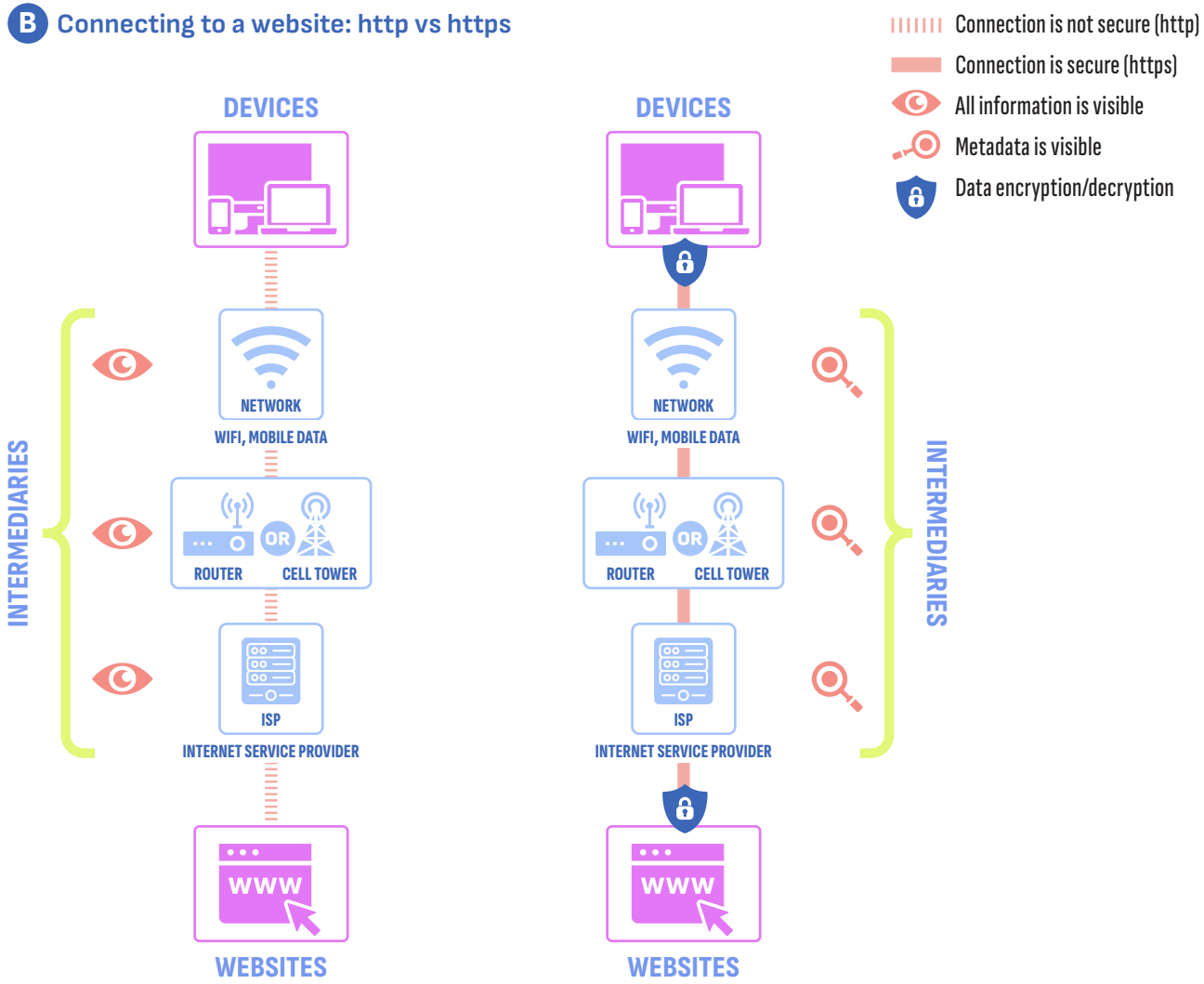
## How can we protect our privacy when accessing websites?

Today, the majority of websites and services use secure connections, which significantly enhance user privacy and data security. In the past, when connections were not secure, every piece of information or data transmitted, including passwords, credit card details, emails, or chat messages, was visible to the administrators of Wi-Fi networks, to ISPs, and to all other intermediaries. This difference can be seen in the use of HTTPS (Hypertext Transfer Protocol Secure) instead of HTTP (Hypertext Transfer Protocol) in web links.

**See DIAGRAM B for an overview of the security difference between http and https.**

When using HTTPS, the intermediaries between our device and a website can only see metadata. For instance, they can see we are visiting youtube.com but cannot identify the specific videos, or facebook.com but cannot identify the profiles viewed. Similarly, they cannot see communication content being sent or received, such as chat messages, emails, passwords, or files.

### B Connecting to a website: http vs https

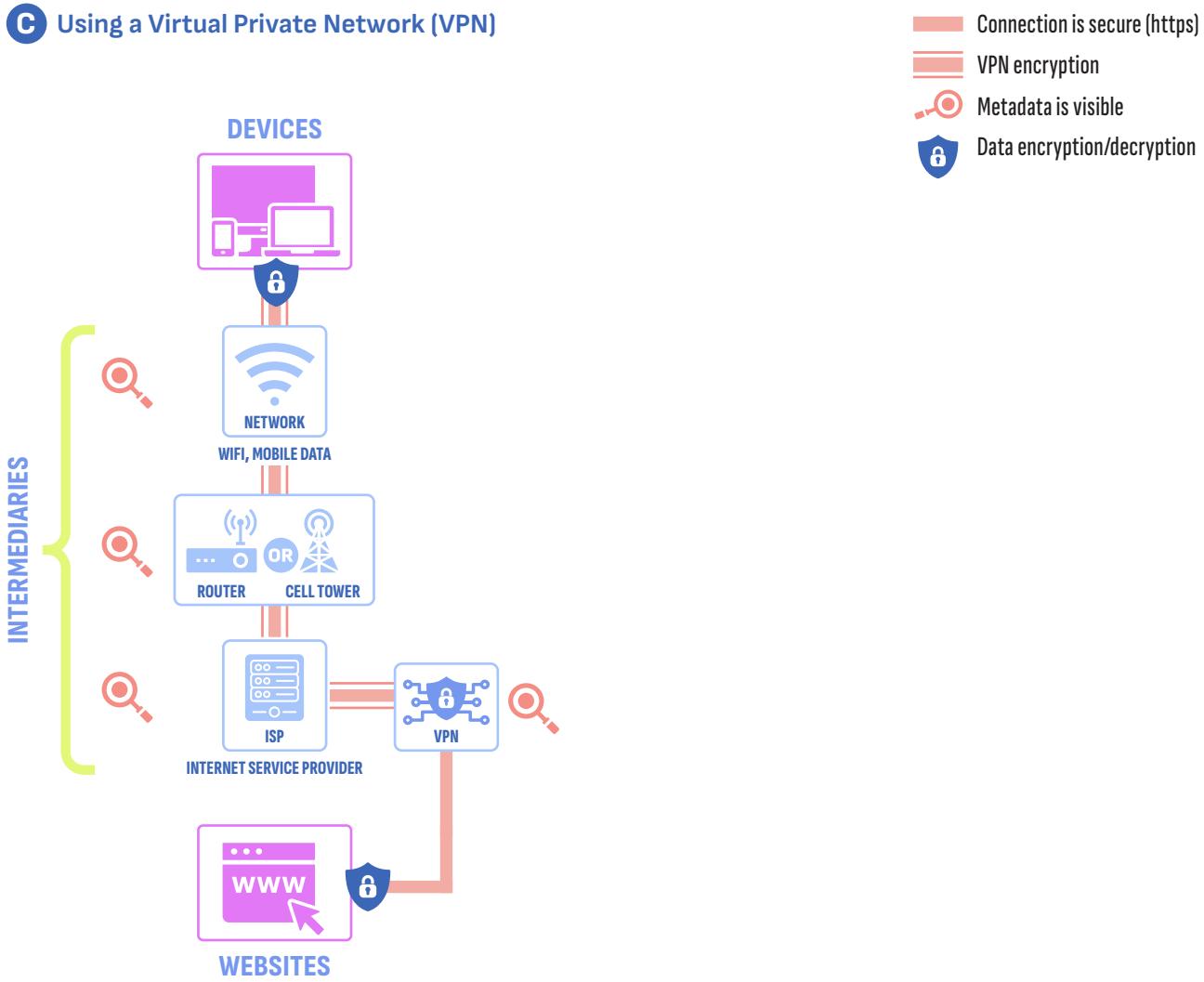


Alongside intermediaries, website administrators can also access significant information about the sites we visit online. They can identify our IP address, browser and device details, all our activity on the site, and all data exchanged. If you have reasons to believe the website is controlled by individuals or organizations with malicious intent towards you, it would be better not to visit such websites or to take some precautions. This could include using a virtual private network (VPN).

**See DIAGRAM C for an overview of how a VPN works.**

To protect our online accounts and communication, it is recommended to use tools and methods, such as two-factor authentication (2FA), access control, and end-to-end encryption (E2EE).

## C Using a Virtual Private Network (VPN)

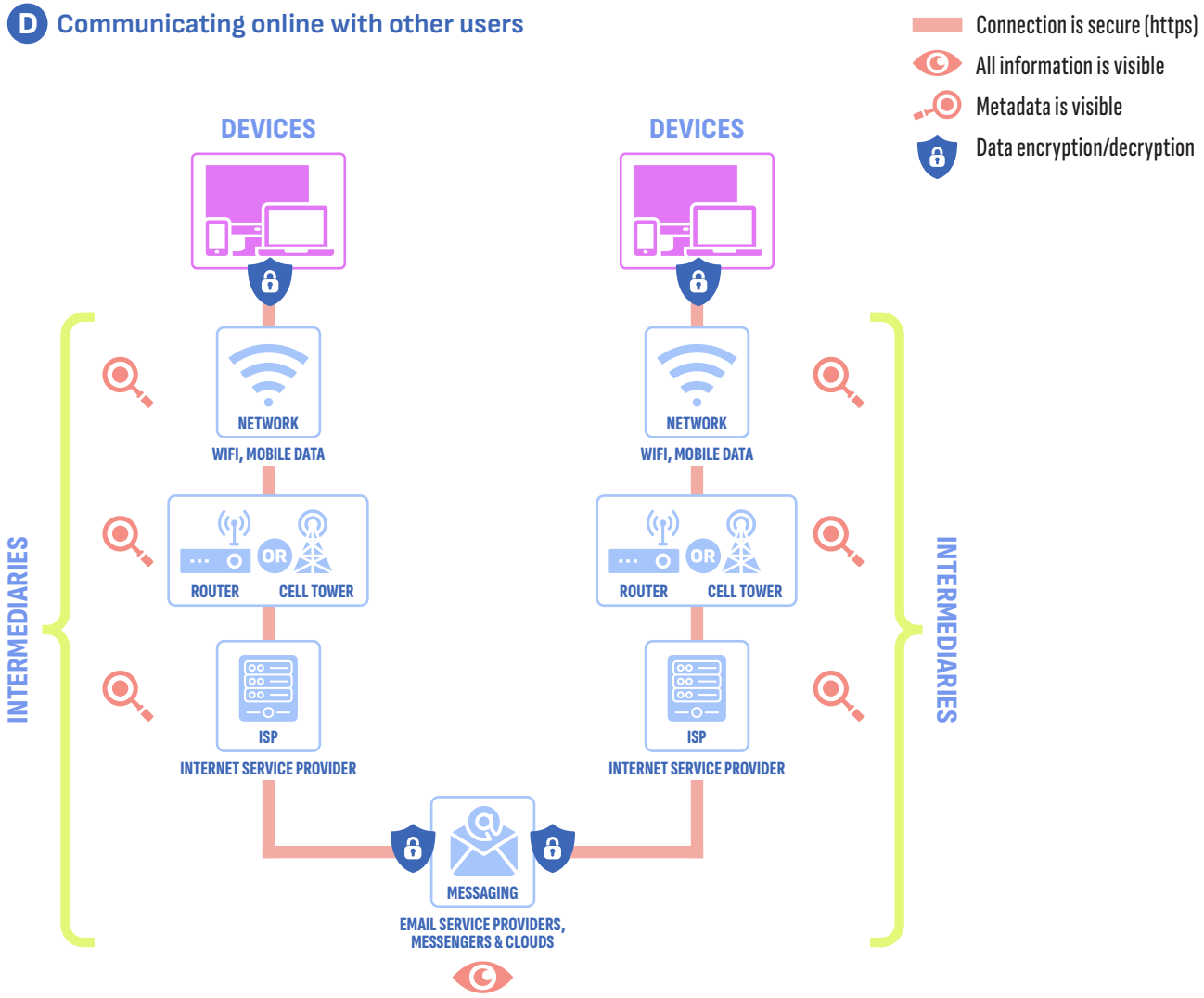


## How can we protect our privacy when using online servers for communicating with other users?

When we send an email through an online service using HTTPS to someone else with the same provider, we can be confident that our connection is secure, meaning Wi-Fi administrators cannot see the content of our email or that we are sending one. However, the email service provider on the other hand can see everything, including the content of our emails, with whom we are communicating, when and how often emails are sent, and from what locations. It is recommended to always check the privacy policy of the services you use to be aware of the types of data or information they can access.

**See DIAGRAM D for an overview of security when communicating with other users.**

### D Communicating online with other users



End-to-end encryption is especially recommended to use when trying to prevent the service provider from seeing our content. Note that despite using end-to-end encryption, which hides what we send and receive, providers can still have access to our metadata.

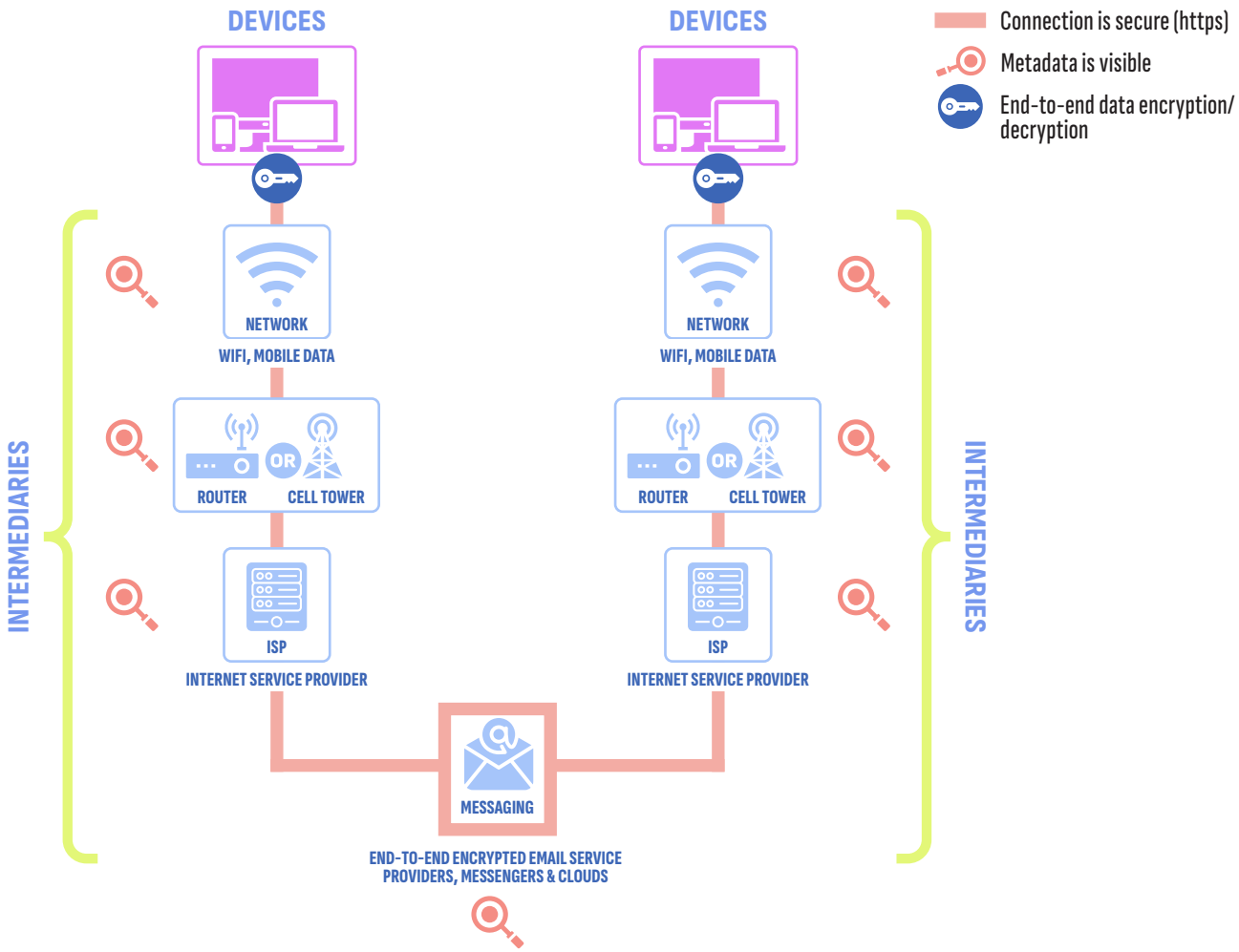
**See DIAGRAM E for an overview of how end-to-end encryption works.**

To assess whether a service provider is secure enough, it is important to understand the legal environment in which the service is based and how it could impact our data security. For instance, certain countries may have laws that allow authorities to access data stored by service providers without your consent.

**Remember to:**

- Avoid the temptation to use every security tool or solution you encounter — security measures must be deliberate, not random.
- Identify and prioritize the main risks and problems before selecting and applying solutions.
- Avoid implementing solutions without understanding which specific issues they address.
- Follow all steps of the risk management process for effective security.

## E Communication online with other users: using end-to-end encryption



# Glossary:

**ACCESS CONTROL:** a method that helps users safeguard their clouds or collaborative spaces by allowing them to manage who can access what. By setting different access levels, users can reduce the risk of data leaks. Each person or entity should only have access to the data and tools necessary for their tasks.

**DATA ENCRYPTION:** a method that prevents third parties from accessing our files by converting the original data into an unreadable form (encryption).

**END-TO-END ENCRYPTION (E2EE):** a private communication system which protects the contents of your messages, texts, and files from being understood by anyone except their intended recipients. No one else, including the communication system provider, telecommunications providers, Internet providers, or malicious actors, can access the data. Encryption turns a clearly readable message into an incomprehensible message that can be decrypted only by the intended recipient.

**FULL-DISK ENCRYPTION:** a method that safeguards all the data on the device by encrypting it, allowing access only to the authorized parties. With full-disk encryption, if someone were to steal or seize the device when it is switched off or locked, they should not be able to access the data.

**MALWARE:** a software intentionally designed to cause harm by accessing and modifying everything on the device, such as stealing data or passwords and spying on its users.

**METADATA:** a digital footprint, including information about our online activities, such as IP address, connection time, traffic volume, and the website's domain.

**PASSWORD MANAGER:** a tool that helps you store passwords. It allows you to remember just one strong password to log into the tool while securely storing the rest.

**PHISHING:** a practice of sending emails or other messages which claim to be from trusted sources but in reality attempt to trick users into installing malware or sharing sensitive information.

**RECOVERY OPTIONS:** a method that allows users who forgot their password to restore access to their accounts. Common recovery options include sending a recovery code to an accessible email account or phone number, back-up codes, or secret questions.

**TWO-FACTOR AUTHENTICATION (2FA):** a method to prove your identity, when logging into accounts, with two or more factors. These factors can be: 1) something you know, such as a password or PIN, 2) something you have, such as a phone, security token, or bank card, and 3) something you are, such as a fingerprint or face recognition.

**VIRTUAL PRIVATE NETWORK (VPN):** a tool that creates a secure connection between your device and a VPN server. Using a VPN hides your IP address, making it appear as though you are browsing from a different location. While your ISP will see you are using a VPN, they will not know which websites you are visiting. Make sure that your VPN provider is trusted by checking, for example, their privacy policy, business models, or even where their servers are located.