What end-to-end encryption is, and why you need it

We explain for laypeople what end-to-end encryption is and how it enables private, secure communication for us all.

Kaspersky Team

- September 11, 2020

In recent years, communications services ranging from WhatsApp to Zoom have announced their implementation of end-to-end encryption. What does that mean? Well, the idea of encryption is pretty straightforward: It turns data into something that cannot be read. But what does *end-to-end* mean? What are its pros and cons? Without getting into the underlying math and technical terms, we'll explain it as simply as we can.

What end-to-end encryption is — and its alternatives

End-to-end encryption is the act of applying encryption to messages on one device such that only the device to which it is sent can decrypt it. The message travels all the way from the sender to the recipient in encrypted form.

What are the alternatives? One alternative is to transfer the data in clear text, that is, without encrypting the message at all. That is the least secure option. For example, data sent by SMS is not encrypted, meaning that in theory anyone can intercept it. Fortunately, in practice, doing so requires special equipment, which somewhat limits who can eavesdrop on your text messages.

Another option is **encryption-in-transit**, whereby messages are encrypted on the sender's end, delivered to the server, decrypted there, re-encrypted, and then delivered to the recipient and decrypted on their end. Encryption-in-transit protects information during transmission, but using it allows the intermediate link in the chain — the server — to see the content. Depending on how trustworthy its owners are, that can be an issue.

At the same time, using encryption-in-transit includes the server in the communication, which opens up a range of services that go beyond simple data transfer. For example, a server can store message history, connect additional participants using alternative channels to a conversation (such as joining a video conference by phone), use automatic moderation, and more.

Encryption-in-transit does solve the most important problem: the interception of data en route from user to server and from server to user, which is the most dangerous part of a

message's journey. That's why not all services rush toward end-to-end encryption: For users gaining convenience and additional services may be more important than adding even more data security.

What end-to-end encryption protects against

The main advantage of end-to-end encryption is its restriction of transmitted data from anyone but the recipient. It is as if when you mailed a letter you put it in a box that was physically impossible to open — immune to any sledgehammer, saw, lockpick, and so forth — except by the addressee. End-to-end encryption ensures the privacy of your communication.

Creating an invincible box isn't really possible in the physical world, but in the world of information it is. Expert mathematicians are constantly developing new encryption systems and improving the strength of old ones.

Another advantage follows from end-to-end encrypted messages being undecryptable by anyone other than the recipient: No one can change the message. Modern encryption methods work in such a way that if someone changes the encrypted data, the message becomes garbled on decryption, making the problem instantly clear. There is no way to make predictable changes to an encrypted message — that is, it's impossible to replace the text.

That ensures the integrity of your communication. If you receive a successfully decrypted message, you can be sure it's the same message that was sent to you and that it wasn't somehow tampered with in transit (in fact, a messaging app will do that for you automatically).

What end-to-end encryption doesn't protect against

After learning about the benefits of end-to-end encryption, readers might get the impression that it's the solution to every information-transfer problem. It isn't, though; end-to-end encryption has limitations.

First, although the use of end-to-end encryption lets you hide the content of your message, that you sent a message to a certain person (or received one from them) will be apparent. The server can't read the messages, but it is definitely aware that you exchanged messages on a certain day and at a certain time. In some cases, merely communicating with particular people may draw unwanted attention.

Second, if someone gains access to the device you use to communicate, they will be able to read all of your messages, as well as write and send messages on your behalf.

Therefore, protecting end-to-end encryption requires the protection of devices and application access — even if only with a PIN code — so that if the device is lost or stolen, your correspondence, along with the ability to impersonate you, does not fall into the wrong hands.

For that reason, devices need to be protected with antivirus software. Malware on a smartphone can read the correspondence on it just as if a living person had physical possession of your phone. That is true regardless of what kind of encryption you use to send and receive messages.

Third and finally, even if you take perfect care of protecting all your devices, and you know for sure no one has access to the messages on them, you can't be certain about your conversation partner's device. End-to-end encryption is no help there.

Despite its limitations, end-to-end encryption is currently the most secure way to transfer confidential data, and that's why more and more communication services are switching to it. That's a good thing.