KEY QUESTION:

HOW DOES INFORMATION TRAVEL THROUGH THE INTERNET IN A SAFE WAY?

HOW DO WE UNDERSTAND THE INTERNET?

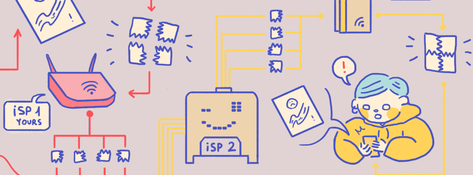
The Internet is not a bubbly cloud. In fact, the internet is a tangible physical system made to move information across the world by using underground or underwater cables. There are many of these cables connecting the world around[1].

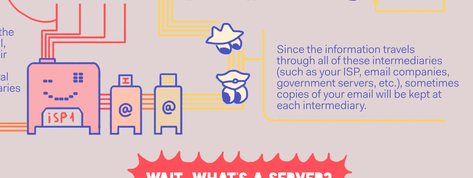
It is possible to send a message from computer A to computer B because both are connected via cables and wireless connection. Our computers can connect wirelessly because they have a technology that allows information to travel through the electromagnetic spectrum.

NOW, LET'S SEE HOW YOUR MESSAGES TRAVEL FROM YOUR COMPUTER TO YOUR FRIEND'S PHONE:

You want to send today an email to Amalia at amalia@gmail.com about the new campaign to protect your community's river. Pressing send takes the mail out of your inbox.

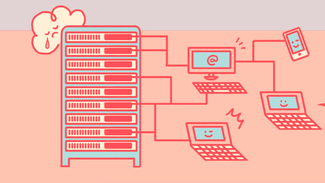
That message breaks into small packages that travel directly to the router, and then over the wires of the Internet Service Provider (ISP).





An ISP can be a private company such as, At&t, Claro, Movistar, B-Mobile, etc., or in certain cases it can be the State.

The message also goes through the infrastructure that Gmail, Hotmail, Yahoo, etc.,; offer, in this case, their servers. This means that your information travels through several intermediate points or intermediaries before it reaches the person you want to talk to.



Since the information travels through all of these intermediaries (such as your ISP, email companies, government servers, etc.), sometimes copies of your email will be kept at each intermediary.

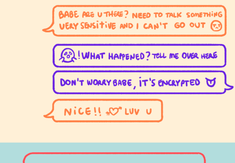
WAIT, WHAT'S A SERVER?

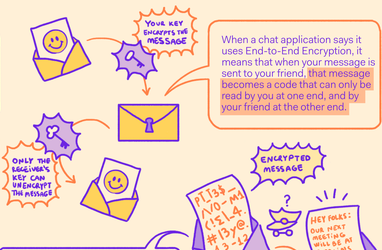
A server is a special computer connected to other computers through cables. The Internet emerges with the interconnection between computers or servers. By uploading and storing your information in the cloud, you are actually storing your information on a server or someone else's computer. Usually the servers belong to private companies or the State.

BUT WHAT TO DO IF YOU DO NOT WANT YOUR INFORMATION TO BE SEEN OR READ BY OTHER PEOPLE OR COMPANIES THAT ARE ON THE INTERNET?

You can use a variety of technologies for that, but one of the ones you may have already heard of is the ENCRYPTION. Encryption allows your message to be encoded with special symbols and letters so it can't be understood by other people.

Have you seen how when you chat on Whatsapp, you are told that your message is protected with an end-to-end encryption? Encryption is very famous in chat applications, but not all of them include it.





When a chat application says it uses End-to-End Encryption, it means that when your message is sent to your friend, that message becomes a code that can only be read by you at one end, and by your friend at the other end.

End-to-end encryption can defend you against surveillance by governments, crackers and the messaging service itself.

IMPORTANT

When you make a call from a landline or cell phone, your call is not encrypted from point to point. When you send a text message (also known as an SMS) on a phone, the text is also not encrypted.

If you are concerned about your messages being intercepted, it may be better to use End-to-End Encryption applications.

End-to-end encryption only protects the content of your communication, not the fact that you are communicating in the first place. It does not protect some of your metadata which includes, for example, the subject line of an email, who you are communicating with and when, or your location.

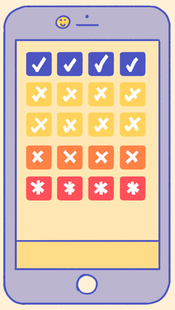
TIP:

Try to use chat applications with end-to-end encryption to protect your information, such as Signal or Wire.

Whatsapp offers this type of encryption, however their internal policies are not reliable.

Some services that do not offer end-to-end encryption by default are: Google Hangouts, Kakao Talk, Line, Snapchat, WeChat, QQ, Yahoo and Messenger.

Some services, such as Facebook Messenger and Telegram, only offer end-to-end encryption if you choose it manually.



LAST MESSAGE:

In this time of pandemic, much of our lives and activism take place on digital platforms. FRIDA |The Young Feminist Fund knows the importance of having safe spaces to organize ourselves as young feminists, and for this reason we decided to bring out a series of contents focused on digital care practices and tools.

The content of this infographic is based on the information developed by organizations that work in digital rights and by hackfeminist collectives. We thank all of them for their efforts to make the internet and technologies safe spaces that help us to continue conspiring together.

References

[1] **Underwater internet cables:** www.submarinecablesmap.com
- **¿Cómo viaja tu información en internet?:** www.youtu.be/SYDWC-qr9mo
- **End to End Encryption:** www.ssd.eff.org/en/module/communicating-others
- **How HTTPS and Tor Work Together to Protect Your Anonymity and Privacy:** www.eff.org/pages/tor-and-https
- **¿Cómo funciona internet?:** www.educacionconsultatotu.com/lessons/modulo-1-como-funciona-internet/
- **How the Internet works in five minutes:** www.youtu.be/7_LPdttKXPc
- **What is the Internet:** www.youtube.com/watch?v=DxcedyqZ73M&feature=youtu.be
- **Introducción a la Criptografía Digital** www.colectivodosiencia.net/herramientas/introduccion-a-la-criptografia-digital/

FRIDA | The Young Feminist Fund
Flexibility Resources Autonomy Diversity Action

youngfeministfund.org
instagram.com/FRIDAFund
twitter.com/FRIDAFund
facebook.com/FRIDAFund