

(<https://encriptados.io/en/>)



7 things you should never do on the internet


 **Pablo Monsalve**(<https://encriptados.io/en/author/pablo/>)

 **May 25, 2022**(<https://encriptados.io/en/blogs/2022/05/25/>)

Connecting to the internet and surfing the web has become part of our daily lives. It is such a normal and day-to-day activity that we often forget that we are running risks and that our data is in danger.

Index

1. **7 things you should never do on the internet** (<https://translate.google.com/website?sl=es&tl=en&hl=es&client=webapp&u=https://encriptados.io/blogs/noticias/7-cosas-que-nunca-debes-hacer-en-internet%23parrafo1>)
2. **Protect your privacy with Encriptados.io** (<https://translate.google.com/website?sl=es&tl=en&hl=es&client=webapp&u=https://encriptados.io/blogs/noticias/7-cosas-que-nunca-debes-hacer-en-internet%23parrafo2>)

 Browsing and communicating through the internet is part of our lives and without a doubt, it has facilitated all day-to-day processes, however there are also risks and dangers to which we are exposed and that we often forget or overlook; That is why today, Encrypted brings you 7 recommendations of things you should never do on the Internet if you do not want to be a victim of cybercriminals or malicious third parties.

7 things you should never do on the internet

1. Do not trust public Wi-Fi networks

Open Wi-Fi networks are extremely dangerous because when you connect to one of them, your data travels freely on the web, leaving it at the mercy of cybercriminals, additionally, many hackers create Wi-Fi networks with common names and the same as the restaurant, bookstore or shopping center that you visit, where when you connect you will be giving personal data to the cybercriminal and in some cases you will even be able to give him control of your devices. So avoid connecting to this type of network and if you must, do not make bank transactions or movements that compromise your personal data.

2. Don't use easy-to-crack passwords

When creating a password, avoid at all costs using your own names, names of relatives or pets, birthdays and obvious data. Always try to use uppercase and lowercase letters, numbers, and characters to make it difficult for cybercriminals and protect all your network and personal information.



3. Avoid using the same password everywhere

A very common mistake is that when we believe that we have created a strong and secure password, we use it everywhere, in social networks, in the mail, in the banking application and any other portal, **me/encriptados** have different passwords for all or at least make some variation to them, if your only password is compromised, all your information and access will be lost.

4. Never click on the links that arrive in your email

All the time we receive emails with advertising, most of which are spam, many times we receive emails supposedly from the bank telling you that your account is blocked and that you must recover it by clicking on a link.

You should avoid doing it at all costs because once you do it you can download malware to your computer or cell phone or be a victim of phishing and you risk having your information and even your identity stolen.

5. Never give your login credentials to anyone

What is the best way to prevent someone from having access to your personal information and data? Simple, that no one has access to these and that is why you should not give keys or access credentials to anyone no matter how much trust you have in them. Prevention is the mother of safety.

6. Count everything you do on social networks

We tend to take our social networks as a diary where we are reporting our movements, our positions, tastes and plans all the time. This is a huge mistake, it doesn't matter if you're not famous, cybercriminals are looking for targets all the time and what better target than a person who is constantly reporting their movements and giving away personal information. Therefore, we must avoid sharing more information on our networks, the less personal and private data we say, the better.

7. Do not accept the default settings of social networks and applications

When we install an application or open an account on a social network, one of the steps that we go through faster and almost without reading are the settings and privacy policies. Something that we should not do, many applications and social networks have items such as location, access to camera or location activated by default, we should read this well and know what we are accepting and thus be able to configure each network or application improving privacy and adjusting them what we want .

Start improving your cybersecurity with these 7 tips and avoid being a victim of fraud. And as an additional plus for complete security, you can purchase any of the products that Encrypted has for you.

×

Telegram

me/encriptados)

Protect your privacy with Encriptados.io



For complete protection on the network, nothing better than using **Encrypted** (<https://translate.google.com/website?sl=es&tl=en&hl=es&client=webapp&u=https://encriptados.io/>) products . You can find the best encrypted cell (<https://translate.google.com/website?sl=es&tl=en&hl=es&client=webapp&u=https://encriptados.io/>) phone brands on the market to have military-grade secure communications and ensure that everything that enters and leaves your mobile phone is encrypted and safe, away from third parties.

You can also find **encrypted applications** (<https://translate.google.com/website?sl=es&tl=en&hl=es&client=webapp&u=https://encriptados.io/>) with strict security policies and extensive features for you to communicate securely and send documents, photos, voice notes with peace of mind and confidence.

And if you are looking for a practical and affordable product, nothing better than the **Encrypted Sim** (<https://translate.google.com/website?sl=es&tl=en&hl=es&client=webapp&u=https://encriptados.io/pages/sim-encriptada-encriptados>) which by simply putting it on your mobile device you will already be giving your communications a strong additional layer of security, not to mention that you can use it in more than 200 countries around the world. .

Don't think about it anymore and start protecting yourself with **Encrypted** (<https://translate.google.com/website?sl=es&tl=en&hl=es&client=webapp&u=https://encriptados.io/>) .

Articulos Destacados



×

How does a DDoS attack work and how to protect yourself from it?
(<https://encriptados.io/en/blogs/news/how-does-a-ddos-attack-work-and-how-to-protect-yourself-from-it/>)

me/encriptados) If you've ever wondered how this type of attack works,

LEER MÁS ([HTTPS://ENCRIPADOS.IO/EN/BLOGS/NEWS/HOW-DOES-A-DDOS-ATTACK-WORK-AND-HOW-TO-PROTECT-YOURSELF-FROM-IT/](https://encriptados.io/en/blogs/news/how-does-a-ddos-attack-work-and-how-to-protect-yourself-from-it/))



× **The best VPN you can use in 2024 (<https://encriptados.io/en/blogs/news/the-best-vpn-you-can-use-in-2024/>)**

Telegram
If you love privacy or simply want to start protecting

LEER MÁS ([HTTPS://ENCRIPADOS.IO/EN/BLOGS/NEWS/THE-BEST-VPN-YOU-CAN-USE-IN-2024/](https://encriptados.io/en/blogs/news/the-best-vpn-you-can-use-in-2024/))

.me/encriptados)



**Disable these functions to avoid being Hacked or Spied on on your Phone
(<https://encriptados.io/en/blogs/news/disable-these-functions-to-avoid-being-hacked-or-spied-on-on-your-phone/>)**

× We know that the security of our data is very

Telegram
LEER MAS ([HTTPS://ENCRYPTADOS.IO/EN/BLOGS/NEWS/DISABLE-THESE-FUNCTIONS-TO-AVOID-BEING-HACKED-OR-SPIED-ON-ON-YOUR-PHONE/](https://ENCRYPTADOS.IO/EN/BLOGS/NEWS/DISABLE-THESE-FUNCTIONS-TO-AVOID-BEING-HACKED-OR-SPIED-ON-ON-YOUR-PHONE/))

.me/encriptados)



eSim: How to stay connected while traveling
(<https://encriptados.io/en/blogs/news/esim-how-to-stay-connected-while-traveling/>)

eSims. The latest innovation in mobile connectivity is revolutionizing the

×

LEER MÁS ([HTTPS://ENCRIP TADCS.IO/EN/BLOGS/NEWS/ESIM-HOW-TO-STAY-CONNECTED-WHILE-TRAVELING/](https://encriptados.io/en/blogs/news/esim-how-to-stay-connected-while-traveling/))
telegram

.me/encriptados)



How to Prevent Ransomware: Strategies to Keep Your Files Safe (<https://encriptados.io/en/blogs/news/how-to-prevent-ransomware-strategies-to-keep-your-files-safe/>)

- × Ransomware is one of the threats that affects the most

Telegram
LEER MAS ([HTTPS://ENCRIPADOS.IO/EN/BLOGS/NEWS/HOW-TO-PREVENT-RANSOMWARE-STRATEGIES-TO-KEEP-YOUR-FILES-SAFE/](https://encriptados.io/en/blogs/news/how-to-prevent-ransomware-strategies-to-keep-your-files-safe/))

.me/encriptados)



Pegasus. This is how the Israeli software used for espionage works.
(<https://encriptados.io/en/blogs/news/pegasus-this-is-how-the-israeli-software-used-for-espionage-works/>)

× The military-grade spy software Pegasus, developed by the Israeli company

Telegram
LEER MAS ([HTTPS://ENCRIPADOS.IO/EN/BLOGS/NEWS/PEGASUS-THIS-IS-HOW-THE-ISRAELI-SOFTWARE-USED-FOR-ESPIONAGE-WORKS/](https://encriptados.io/en/blogs/news/pegasus-this-is-how-the-israeli-software-used-for-espionage-works/))

.me/encriptados)

Suscríbete a nuestro Blog

He leído y acepto los [Términos y condiciones](https://encriptados.io/pages/terminos-y-condiciones/) y la [Política tratamiento de datos](https://encriptados.io/pages/politica-de-tratamiento-de-datos/).

Suscríbete



(<https://encriptados.io/pages/sim-encriptada/>)



Answer these 6 questions and determine if you are protecting the information on your mobile device

Download Free

×

Secure payment

Telegram

[me/encriptados](https://encriptados.io))



Encrypted Cell Phones

- [Cryptcom\(/en/pages/cryptcom/\)](#)
- [Chatmail\(/en/pages/chatmail/\)](#)
- [GhostChat\(/en/pages/ghost-chat/\)](#)
- [VaultChat\(/en/pages/vaultchat/\)](#)
- [Renati\(/en/pages/renati/\)](#)
- [Secure MDM iPhone\(/en/pages/secure-mdm-iphone/\)](#)
- [Secure MDM Android\(/en/pages/secure-mdm-android/\)](#)
- [T2 Communicator\(/en/pages/t2-communicator/\)](#)

Encrypted Cell Phones

- [Secure Crypt\(/en/pages/securecrypt/\)](#)
- [Armadillo\(/en/pages/armadillo-phone/\)](#)
- [UltraX\(/en/pages/ultrax/\)](#)
- [Tribu\(/en/pages/tribu-phone/\)](#)
- [Intact\(/en/pages/intact-phone/\)](#)
- [DEC Secure\(/en/pages/dec-secure/\)](#)
- [TotalSec\(/en/pages/totalsec/\)](#)

×

Telegram

Encrypted Apps





- [Silent Circle\(/en/pages/silent-circle/\)](#)
- [Vnclagoon\(/en/pages/vnclagoon/\)](#)

- [Threema\(/en/pages/threema-app/\)](/en/pages/threema-app/)
- [Threema Work\(/en/pages/threema-work/\)](/en/pages/threema-work/)
- [NordVPN\(/en/pages/nordvpn/\)](/en/pages/nordvpn/)
- [Salt\(/en/pages/salt/\)](/en/pages/salt/)
- [VaultChat\(/en/pages/vaultchat-app/\)](/en/pages/vaultchat-app/)
- [Armadillo\(/en/pages/armadillo-chat/\)](/en/pages/armadillo-chat/)

Contact us by Telegram



@ENCRIPADOS

-  (https://twitter.com/encriptados_io)  (https://t.me/encriptados_english)
-  (<https://www.linkedin.com/company/encriptados-english/>)
-  (<https://www.youtube.com/playlist?list=PLXwHdqNedAjoAwzhnlEgyDdPS08qzMvej>)
- • • (<https://encriptados.io/redes-sociales/>)



[Terms and conditions \(https://encriptados.io/en/pages/terms-and-conditions/\)](https://encriptados.io/en/pages/terms-and-conditions/) | [Data treatment policy \(https://encriptados.io/en/pages/data-processing-policy/\)](https://encriptados.io/en/pages/data-processing-policy/)

×

Telegram



([https://www.dmca.com/Protection/Status.aspx?ID=d2b73015-069d-4421-a52a-960370bdc9bd&refurl=https://encriptados.io/en/blogs/news/7-things-you-should-](https://www.dmca.com/Protection/Status.aspx?ID=d2b73015-069d-4421-a52a-960370bdc9bd&refurl=https://encriptados.io/en/blogs/news/7-things-you-should-never-do-on-the-internet/)

[me/encriptados](https://www.dmca.com/Protection/Status.aspx?ID=d2b73015-069d-4421-a52a-960370bdc9bd&refurl=https://encriptados.io/en/blogs/news/7-things-you-should-never-do-on-the-internet/))

×

Telegram

.me/encriptados)