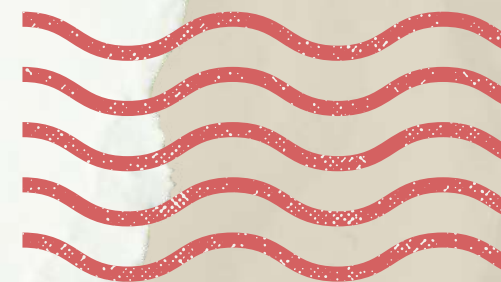




..... 's Booklet
for Using ICT Tools

Created by the partners of
Project "DIGITALIZE – tools for Roma adults
to use the internet and promote education"

Partner Organizations:





- My Booklet for Using ICT Tools -

Project "Digitalize - tools for Roma adults to use the internet and promote education"

This document was created within the frameworks of the "Digitalize - tools for Roma adults to use the internet and promote education" project implemented by Amaro Foro e.V., Együttható Egyesület, Nevo Parudimos, and RROMA. The project is supported by the Erasmus+ programme of the European Union. Project number: 2020-1-DE02-KA227-ADU-008321. The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Author: YOZKAN, Pelin - Együttható Egyesület

Co-funded by the
Erasmus+ Programme
of the European Union



- Table of Contents -

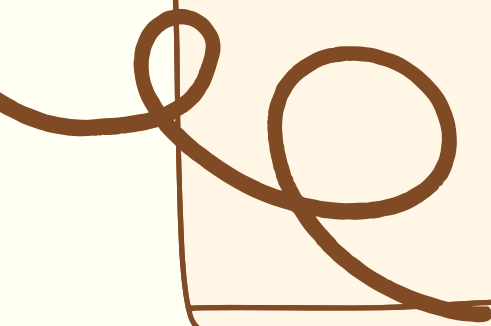
STAY SAFE ON
SOCIAL MEDIA

DATA PROTECTION
& DIGITAL
FOOTPRINT

CYBER-
BULLYING &
ONLINE HATE
SPEECH

ONLINE SHOPPING
AND BANKING

ONLINE
ACCESS TO
SERVICES





Here are our top 10 tips
to stay safe on social
media:

Tip 1

Use a strong password

Make your passwords unique!

Use a different password for each of your online accounts. Reusing passwords is risky!



Facebook



Instagram



Tiktok

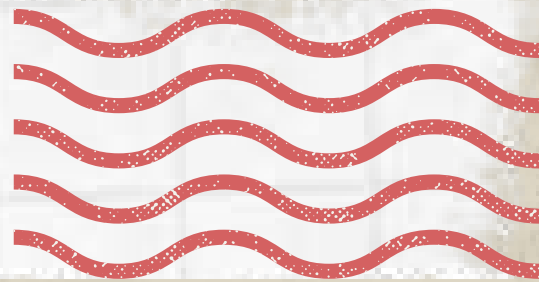


Bank account

If someone gets your password for one account, they could access your email, address, and even your money.

Tip 1

Use a strong password



Make your password longer & more memorable!

Long passwords are stronger, so make your password at least 12 characters long.

 * * * * * * * * * * * * * *

 * * * *

Try to use:

- A lyric from a song or poem
- A meaningful quote from a movie or speech
- A series of words that are meaningful to you
- An abbreviation: Make a password from the first letter of each word in a sentence.

password123

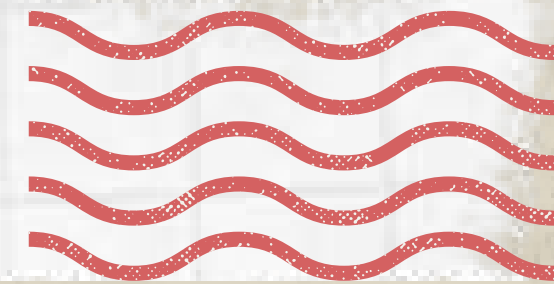


evaluator-passenger-whoops-ablaze



Tip 1

Use a strong password



Don't use
personal info!

Avoid personal info & common words!

Don't create passwords from info that others might know or could easily find out (like the accessible info in your social media profile).

Such as,

- Your nickname or initials
- The name of your child or pet
- Important birthdays or years
- The name of your street
- Numbers from your address



Tip 1

Use a strong password

Don't use common, simple words, phrases & patterns that are easy to guess!

Examples:

- Obvious words and phrases like "password" or "yourname"
- Sequences like "abcd" or "1234"
- Keyboard patterns like "qwerty" or "qazwsx"

My password

~~123456~~

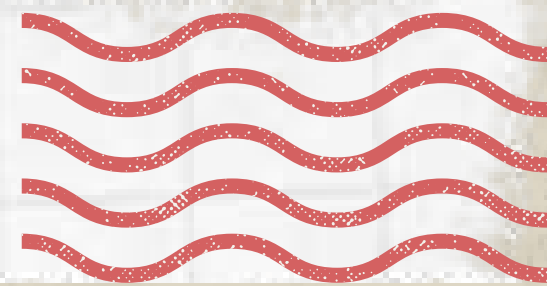
~~qwerty~~

A3eT8M6BFI





Use a strong password



Keep passwords secure!

After you create a strong password, take steps to keep it safe:

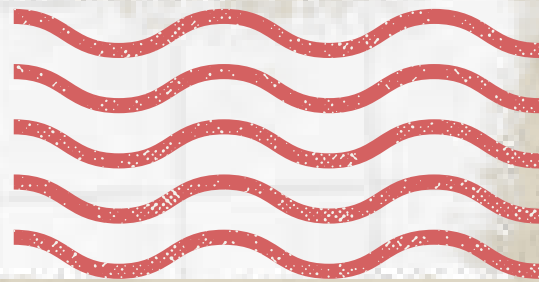
Step 1. Hide written passwords:

If you need to write your password down to remember, don't leave it on your computer or desk. Make sure any written passwords are stored somewhere that's secret or locked.

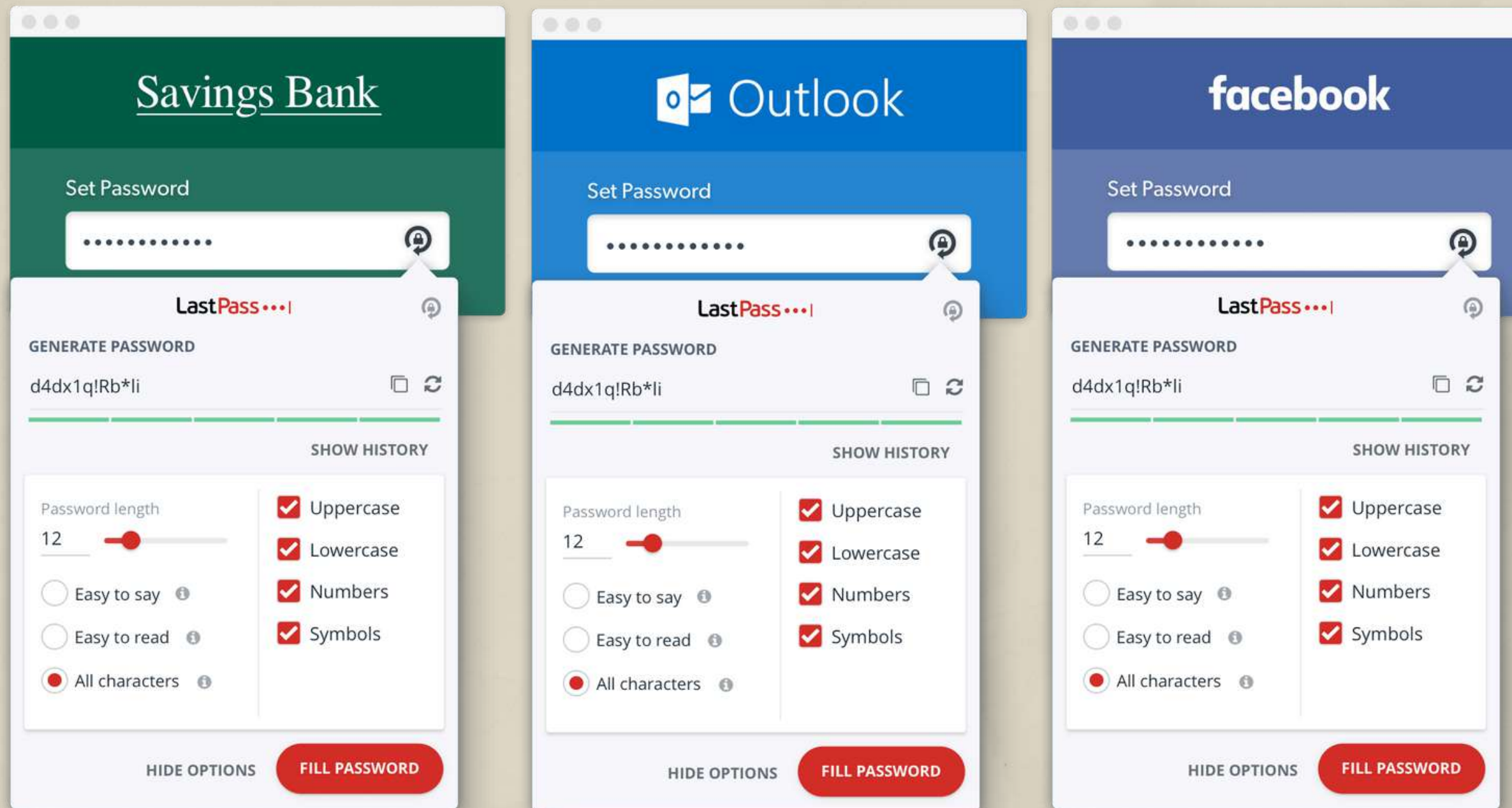


Tip 1

Use a strong password



Step II. Manage your passwords with a tool:



One way to store and remember passwords securely is to use a tool that stores your list of usernames and passwords in encrypted form. Some of these tools will even help by automatically filling in the information for you on certain websites. (Example: LastPass.)

Tip 2

Protect your device with a password

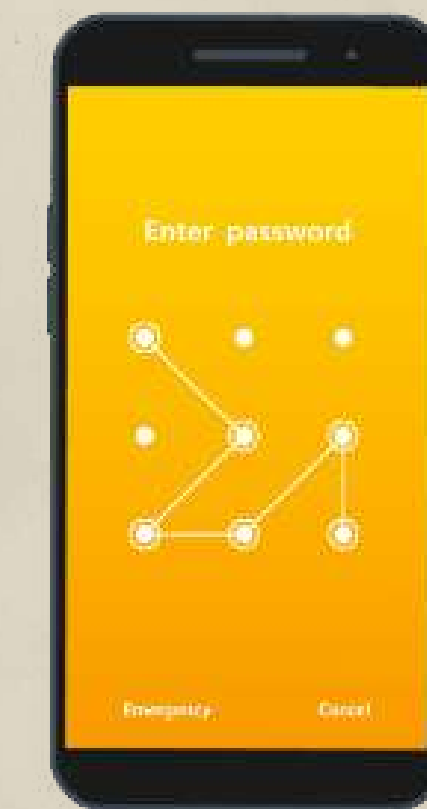
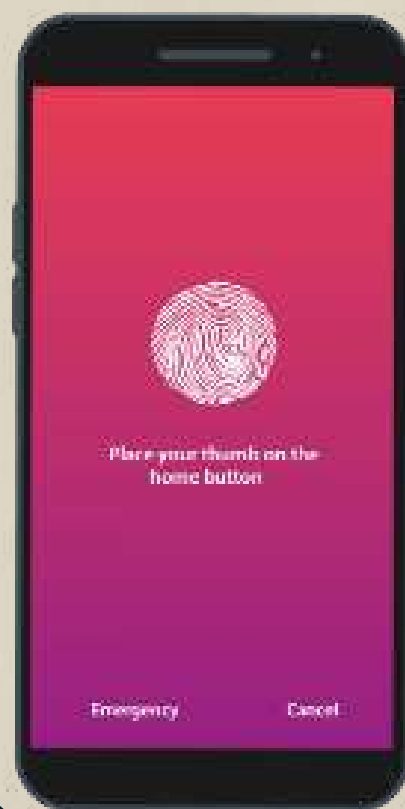


Setting a passcode on your mobile device will help keep unauthorized users off of your device and can help if your device is ever lost or stolen. Each time you turn on or wake up your device, it will ask you for your passcode before you can use the device. Under the "Security" section of your smart device, you are presented with several lock type choices:

Facial Recognition - you can show your face to confirm your identity. It simply recognizes one person as the sole owner of the device, while limiting access to others.



Fingerprint Recognition - It's another form of biometric security such as face recognition.



PIN - you can enter a 4 digit (6 digit on some devices) code to unlock your device

Pattern - you can draw a pattern on a grid to unlock your device

Tip 3

Keep Your Device Updated



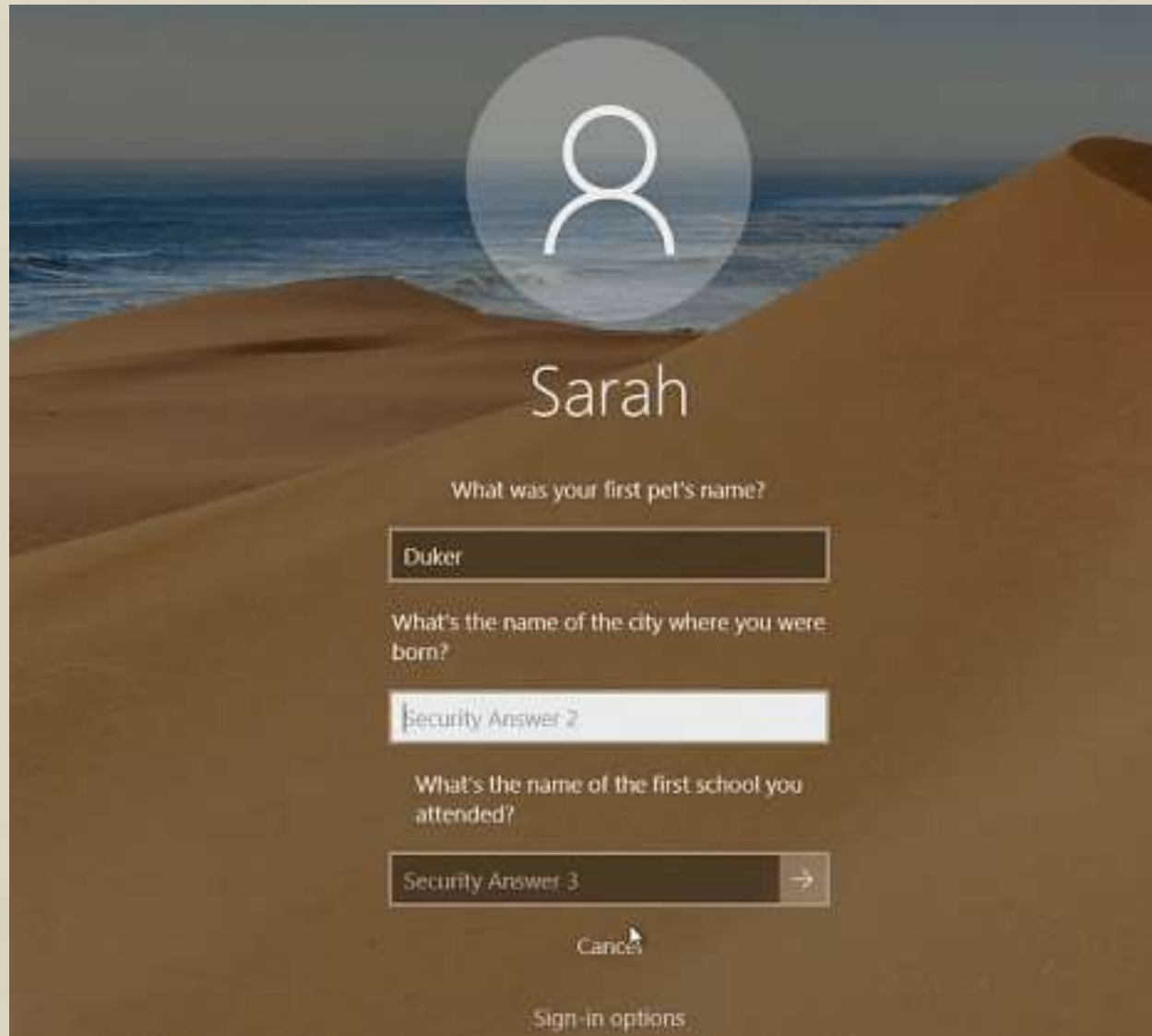
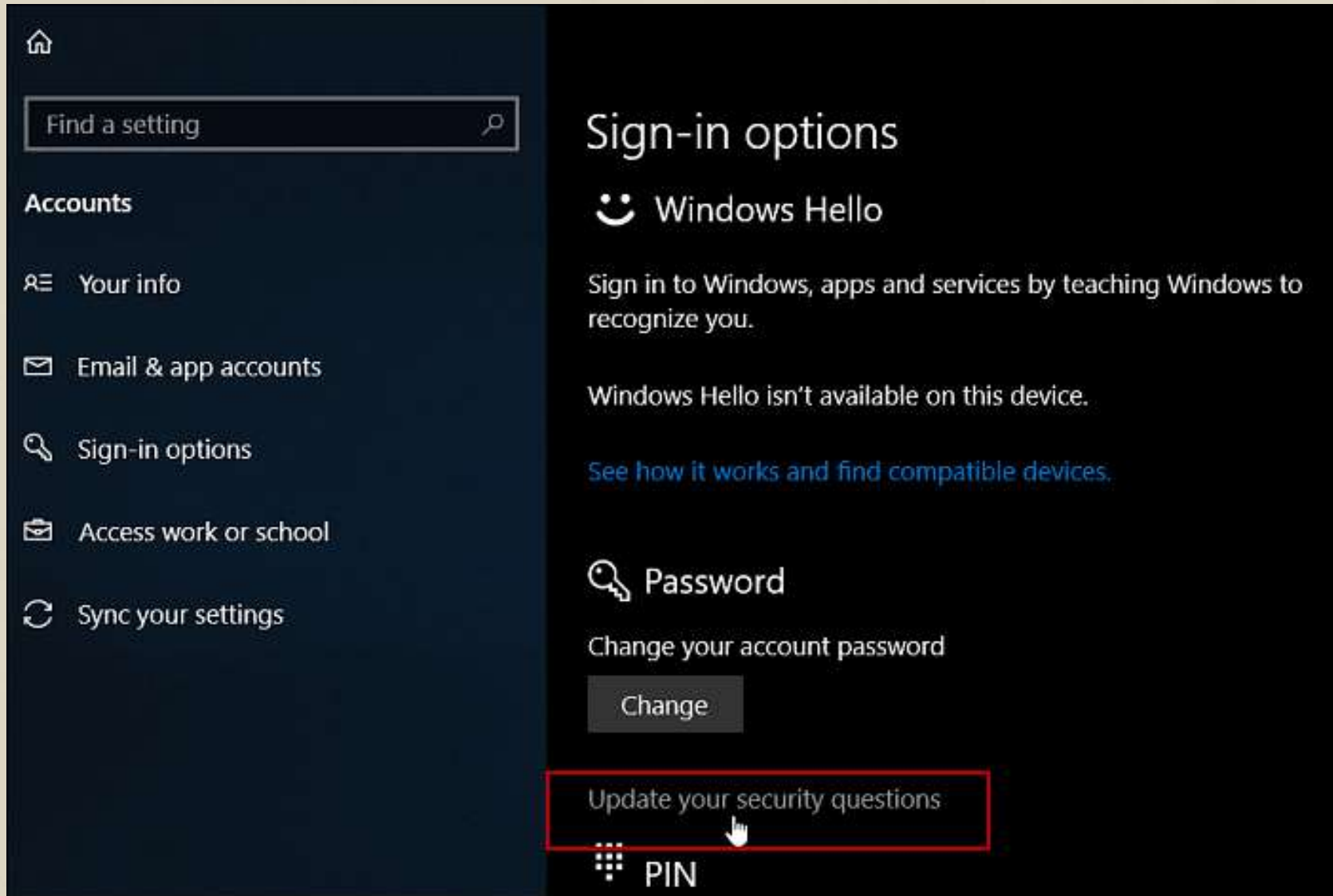
Computer developers release updates to keep products safe. Keep your device software up to date so it is not vulnerable to malware.

Also, protect your computer by installing antivirus software to safeguard.



Tip 4

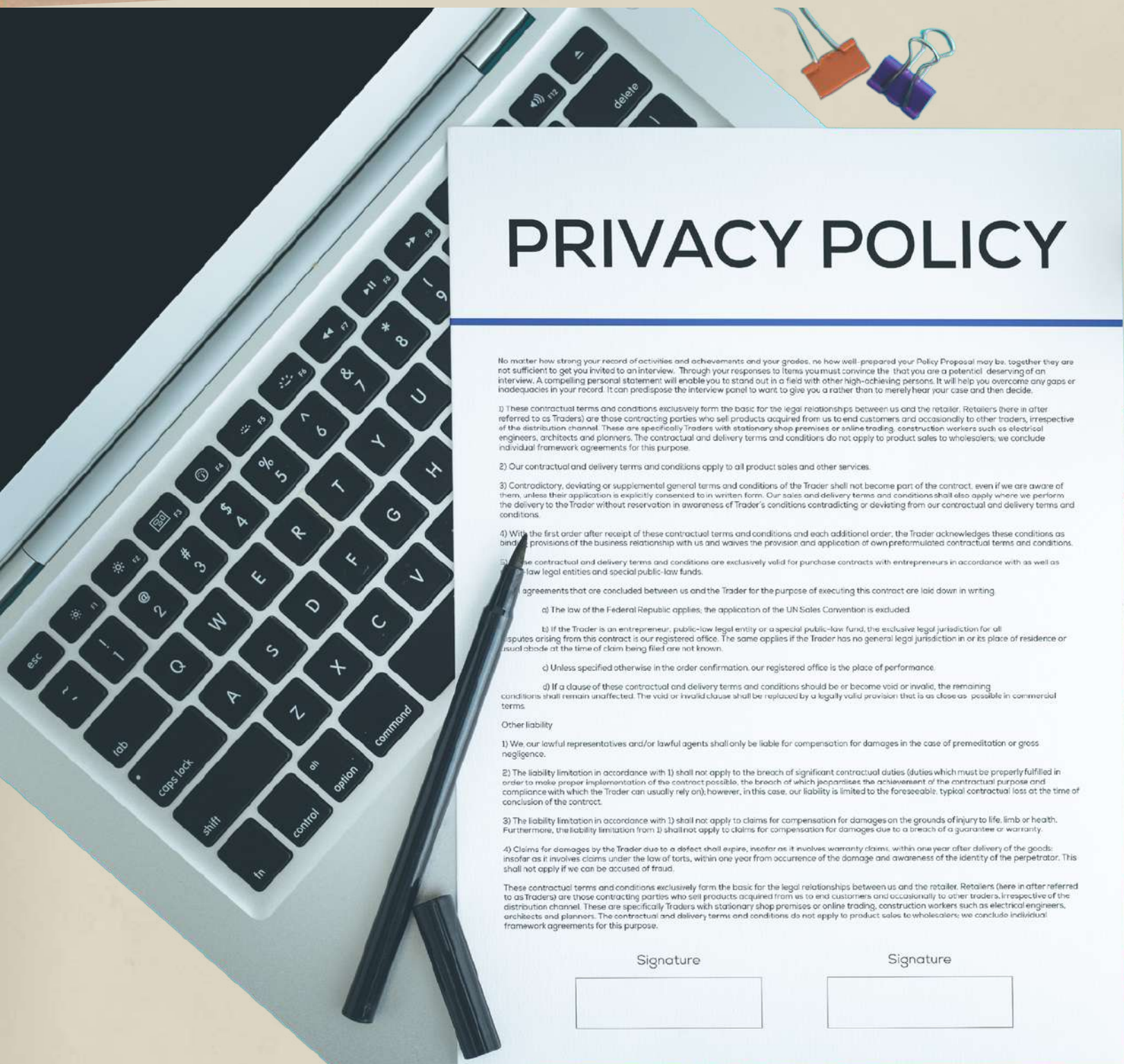
Set up your security answers



Security questions are made to ensure the safety of your user account. They are also used to identify you if you forget your password and cannot access your account. This option is available on most social media sites.

Tip 5

Learn the privacy settings

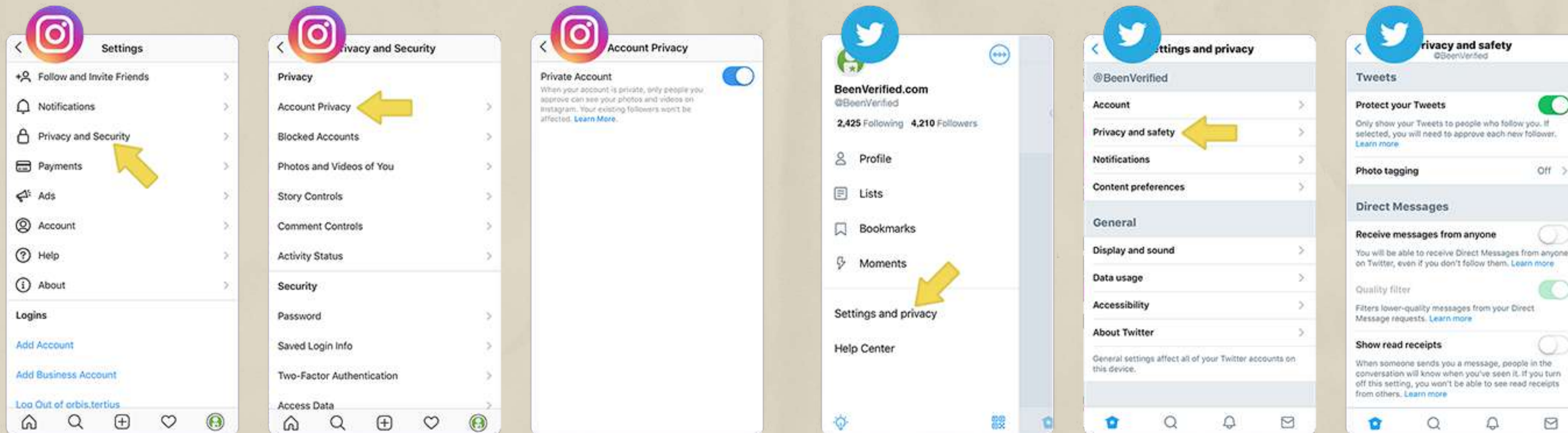


Become familiar with the privacy policies for any device, app, or service you use!

Some apps will ask for permission to access photos and other personal information. Stay informed so you aren't sharing anything you don't want to.

Tip 6

Set your profiles to private



Think carefully about whom you want to see your posts & shared personal info with. Consider setting your profiles to **friends/followers only**. When you set your profile to private, only accepted followers have access to the content you post.

Tip 7

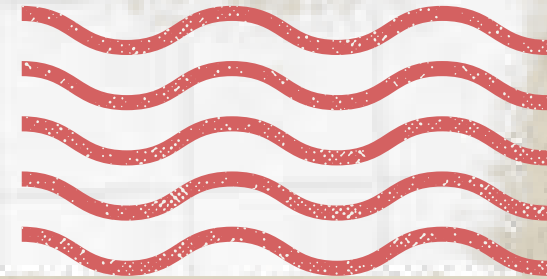
Be careful about what you share



Even with strong privacy settings in place, it is important that you come to terms with the fact that what you post online is never really private and can be shared. It is therefore important that you always **think before you post.**

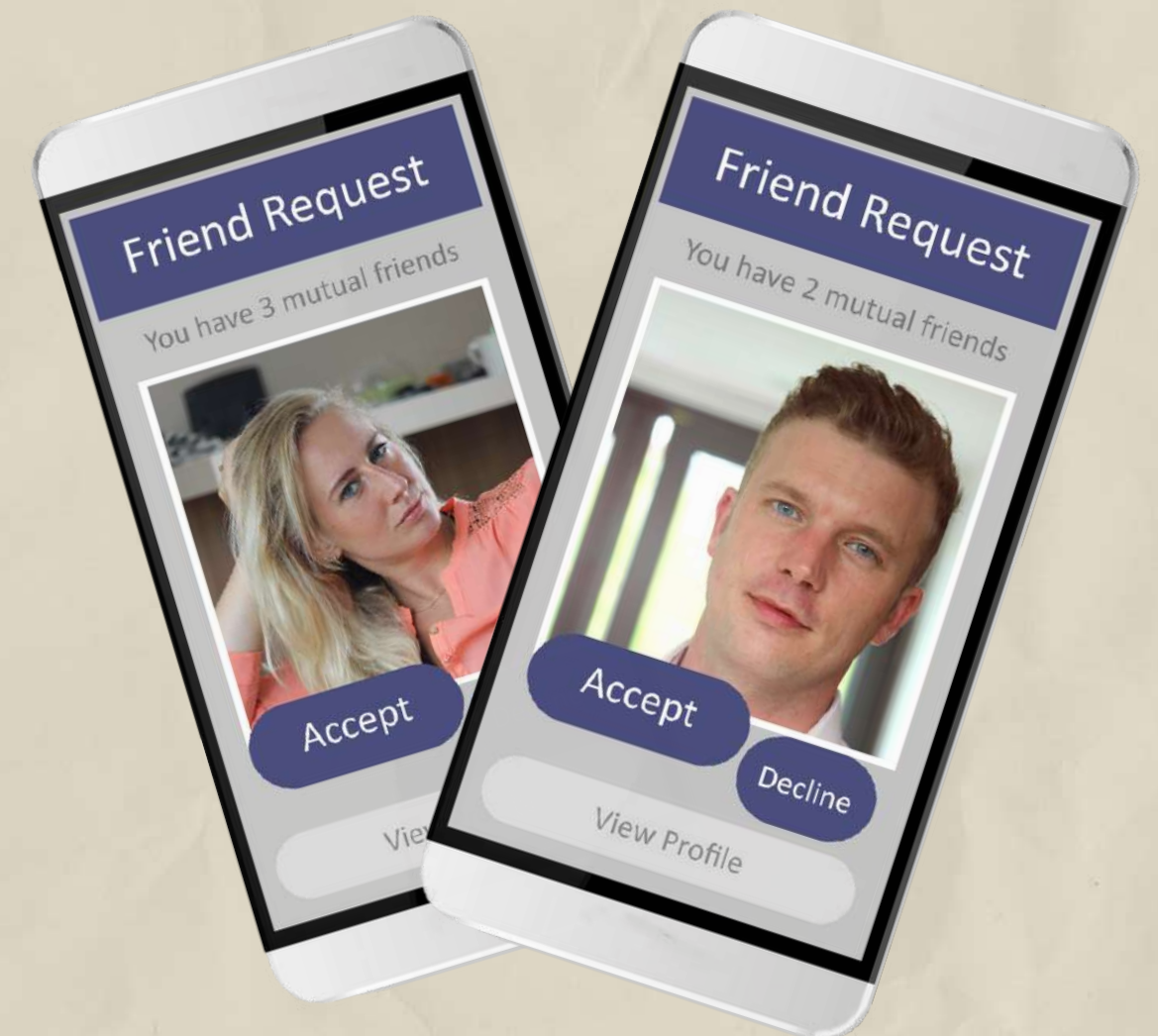
Tip 8

Be selective with friend requests



If you don't know the person, don't accept their request!

Even if you do, click over to their profile to make sure it's not a fake account trying to access your sensitive information. Cybercriminals may impersonate people you know online. They can be set up to scam people out of money, push political propaganda, or any number of other nefarious reasons.



Tip 9

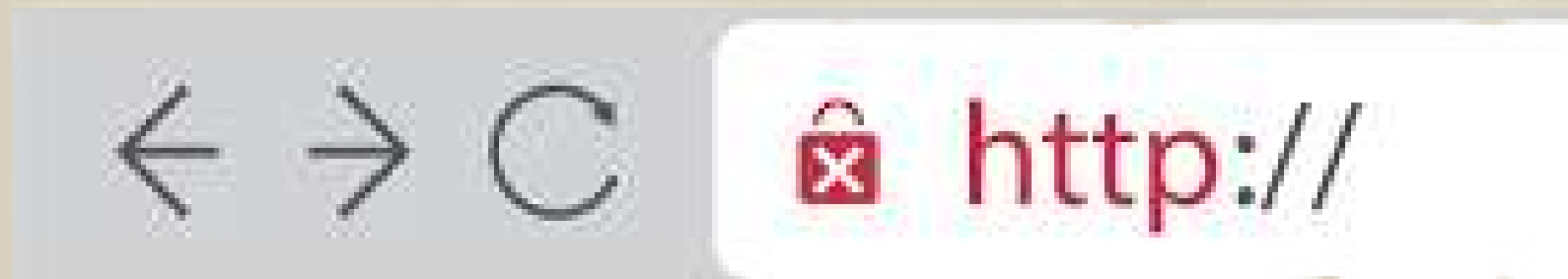
Click links with caution

Be careful of websites or emails containing suspicious links. Some websites may use quizzes, freebies, or salacious stories to get you to click on them and then steal your personal information.



Check Website Reliability!

You can do this by checking if it has a small lock icon or "https" before the URL. The "s" in "https" stands for "secure" and the lock means it's confirmed as a safe site by your browser.

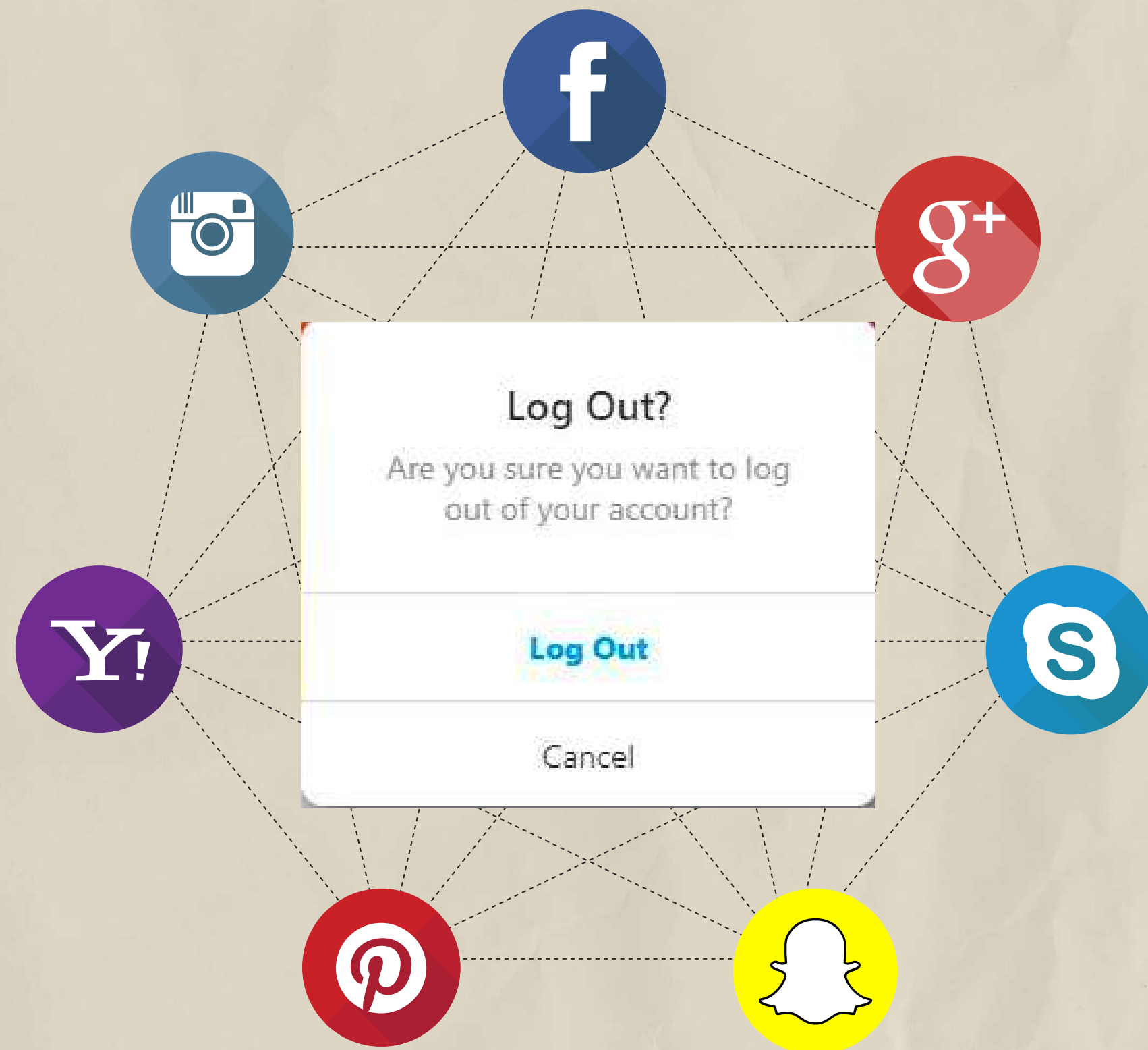


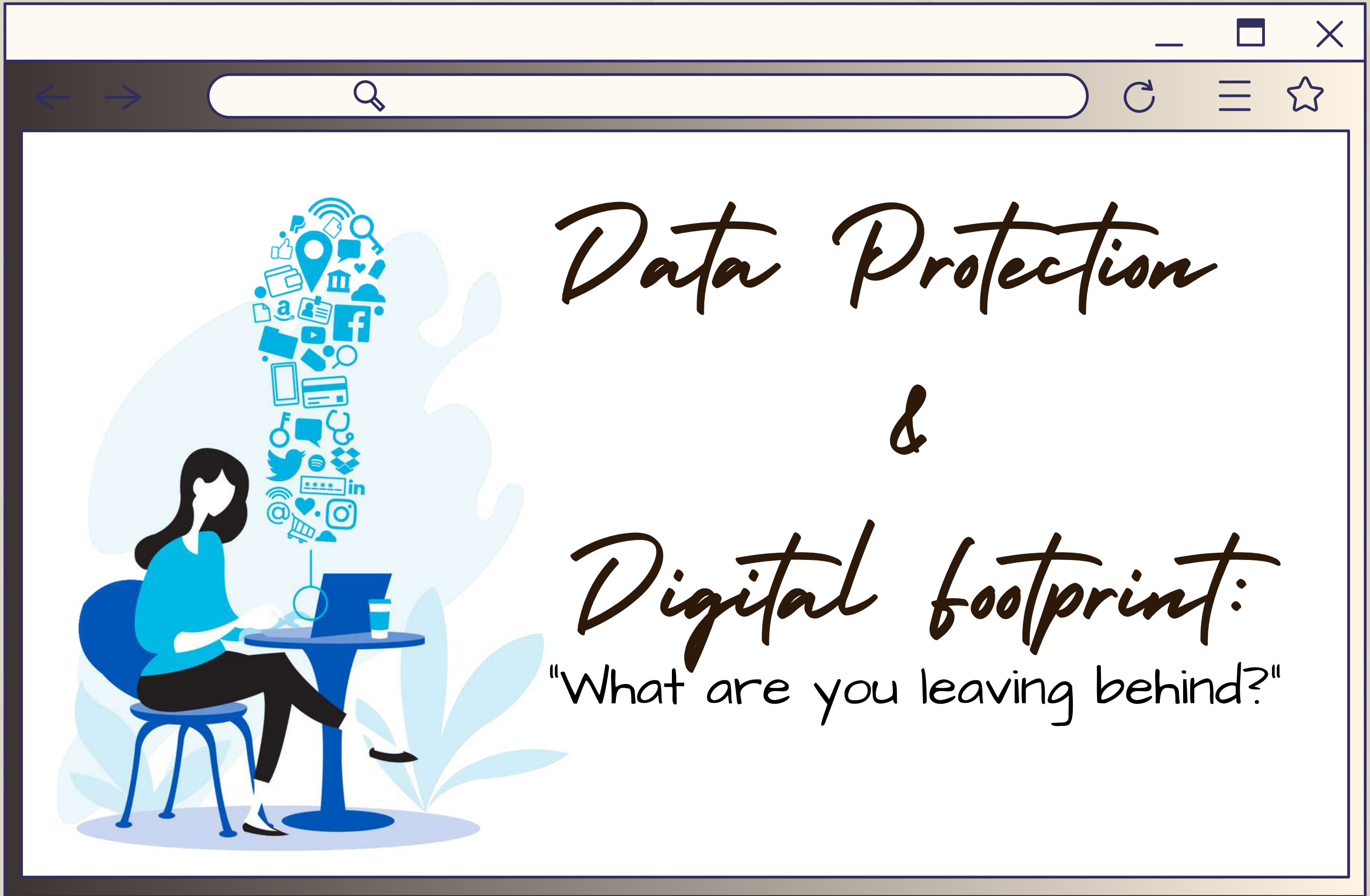
Tip 10

Log out when you're done



Don't let your browser remember your log-on details. It's much safer to re-enter your details every time you log on, even if it takes slightly longer.





Data Protection

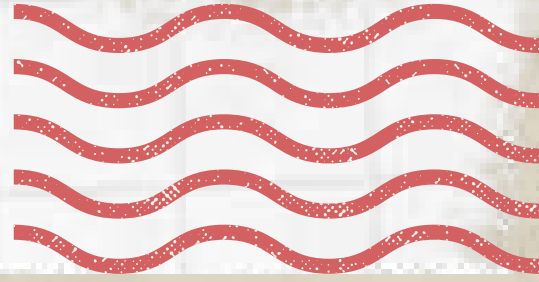
&

Digital footprint:

"What are you leaving behind?"



What is Digital Data?



Data: "The information stored on a computer system"

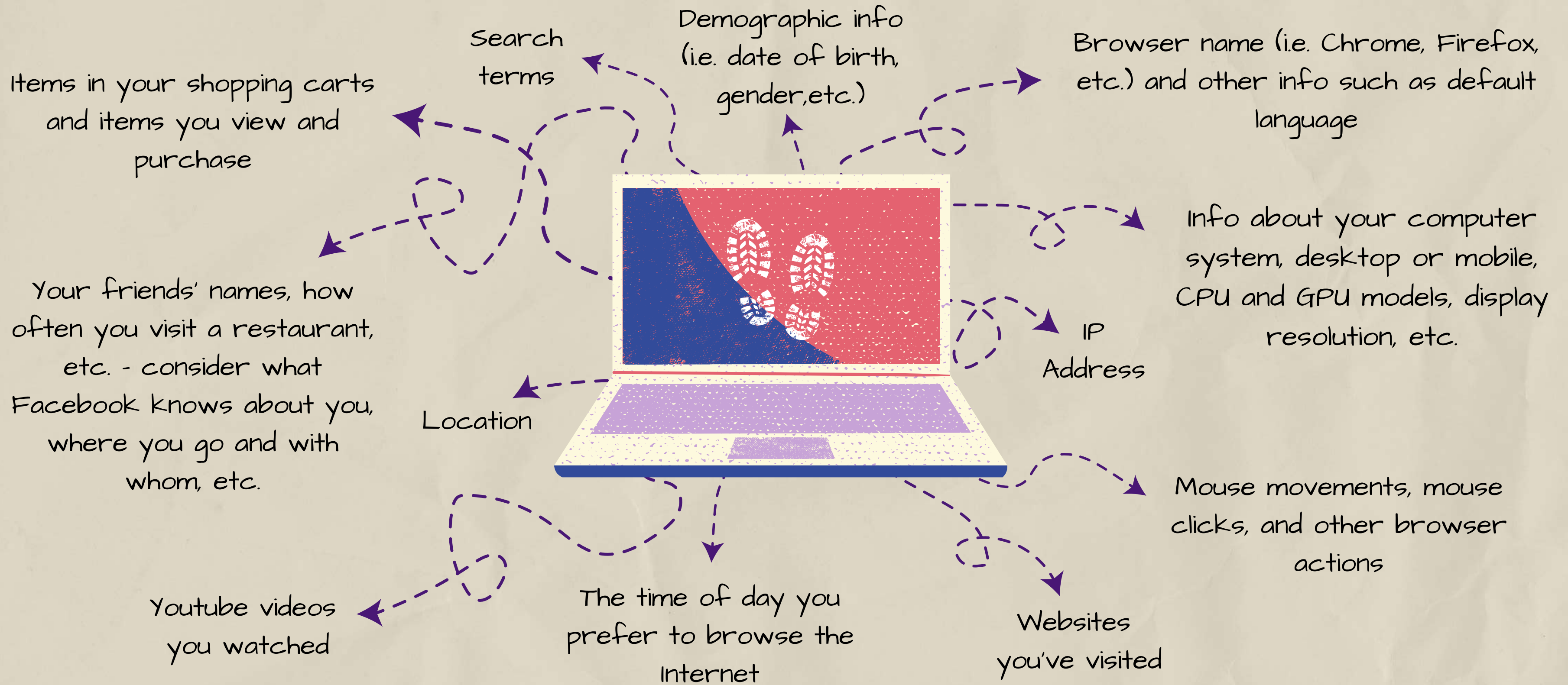
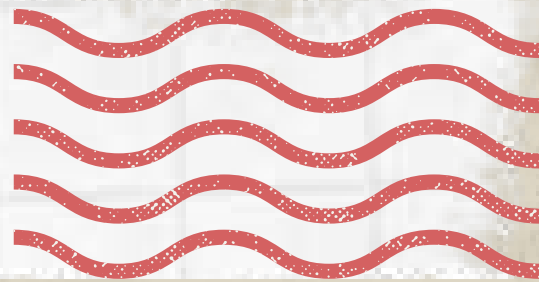
Even though digital platforms market themselves as "free" - they are not. Social media companies are making a profit from data mining - users pay for the services with their own data and their privacy.

The aim of these companies is that make everyone share information as much as possible about themselves and to collect as much data as possible about everyone. And they turn these data into databases for efficient, well targeted advertisements.



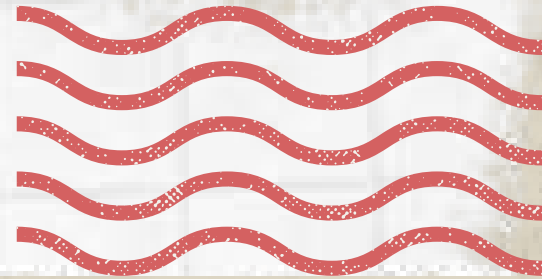


What Data is Collected from You as You Browse the Internet?





How to manage your digital footprint?



Digital Footprint: "What you are leaving behind."



A "digital footprint" is basically your entire online presence—all of the information, posts, pictures, and data you put online, whether purposely or not. The more information you put online, the more people can learn about you. Some people can use that information to determine what you might be interested in buying, or for other less savory purposes such as trying to hack into our online accounts and trying to access passwords, banking information, etc.



How to manage your digital footprint?



Digital footprints including the meta data and content does impact on security, privacy and trust. As the internet becomes bigger and bigger it is becoming increasingly important to think about what might happen to the ownership of the photos that you own and content that you write. You may even be the target of digital identity theft.



Remember that what goes on the internet normally stays there even if you do delete posts there will be a trail of data that you have left behind.



Here are the top 10 things that can be done to reduce and manage your digital footprint





How to manage your digital footprint?



1. Search yourself online to see what comes up.



You have to know exactly what your digital footprint is to manage it well. Search for yourself on a few different search engines (Google, Yahoo, etc.) to see the results that come up. Make a list of anything that you'd like to get rid of or improve.



How to manage your digital footprint?



2. Set a Google alert for your own name!

That way, you'll get a notification if anything mentioning you appears online. You can't always control what shows up online by yourself. For more help, contact the search engine that the results show up on and ask them to delete it. For example, Google allows you to report personal or private information showing up on their search engine by visiting the **Google**

Support page.

Google Alerts

Search query:

Result type:

How often:

How many:

Deliver to:

CREATE ALERT

.....→ Type your name here!



How to manage your digital footprint?



3. Shut down profiles or accounts you don't use anymore, and set your account options to private.

There's no point in keeping accounts that you don't use. Having all these accounts open just increases the amount of information about you online. This clutters your online presence, so close or delete any accounts that you don't use anymore.

Plus to that, adjust the settings to private on all of your remaining platforms to control and limit who can see your posts.

Delete Account

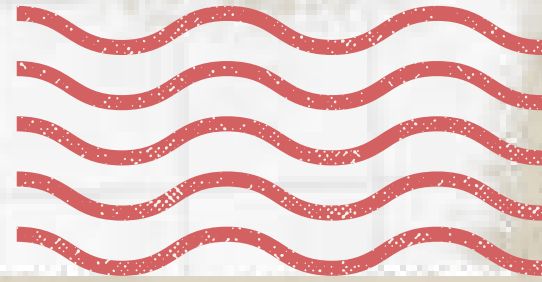
Are you sure you want to delete your account? This will permanently erase your account.

Cancel

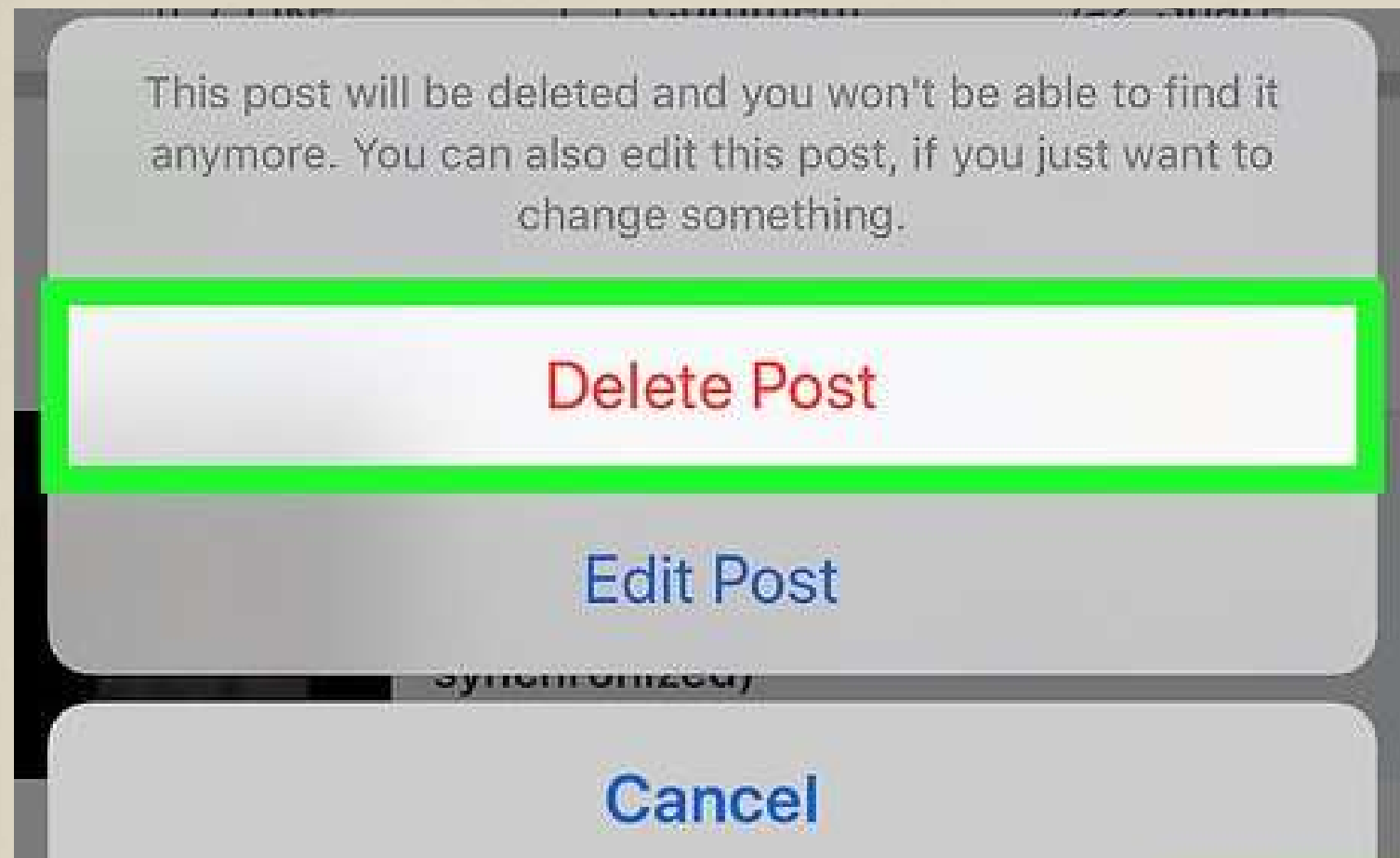
Delete 



How to manage your digital footprint?



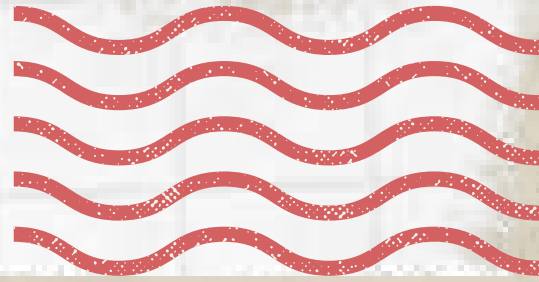
4. Delete anything that doesn't portray you well.



You might find some unprofessional posts when you search for yourself. This means that anyone can potentially see them, which could hurt you in your personal and professional life. Generally, questionable content includes profanity, risqué photos, drinking, or rude comments. Delete these if they show up, and resist posting more in the future.



How to manage your digital footprint?



5. Think before you post.

Think about all the implications of the posts you made, and only share things that show you in a positive, professional light. Try to avoid posting something if you're feeling emotional or angry. You might not be thinking about the bigger implications of what you say.

Remember that using privacy settings is not a substitute for being careful about what you post. Still avoid making inappropriate posts, even if your accounts are locked down.

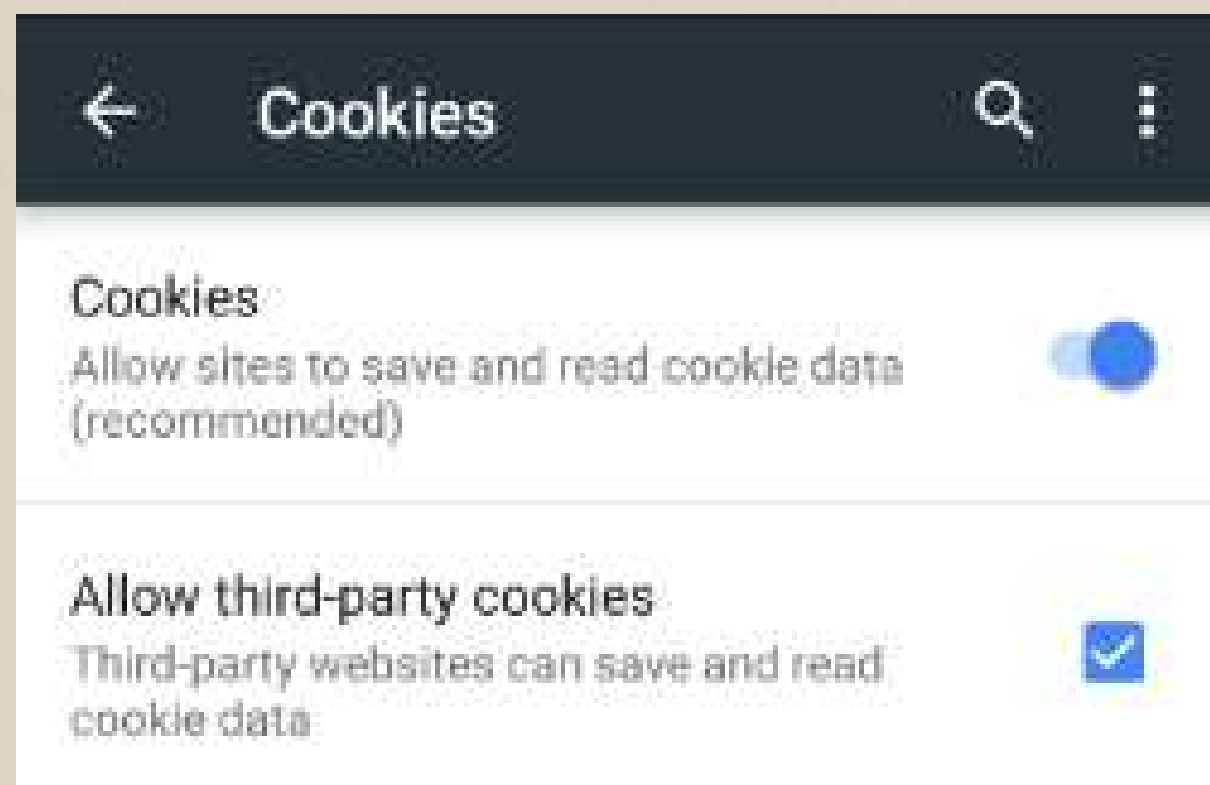




How to manage your digital footprint?



6. Delete cookies every few months to clear tracking data.



Cookies are used to track your search data for specific sites. This is supposed to make your web experience more convenient because sites will remember you, but it could also store your personal information.

To avoid this, make a habit of clearing the cookies on your web browser every few months to get rid of anything that could be tracking your activity.





How to manage your digital footprint?



7. Watch out for suspicious messages and phishing emails.

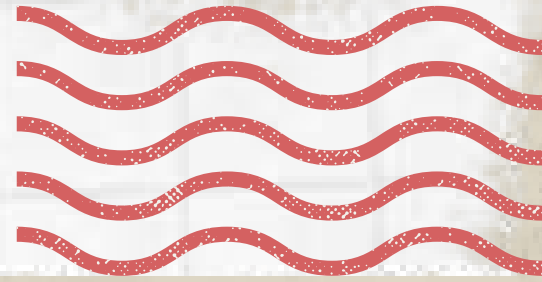
Messages with a shortened URL alongside a statement such as 'OMG look at this picture of you...' or 'Have you seen what they are saying about you...' are not to be trusted. Don't click links that come in those texts.



Phishing emails are also a problem. These are fake communications pretending to be a trusted organization such as Facebook that will try and get you to log in and stole your data.



How to manage your digital footprint?



8. Recognize the fakes.

Not everyone on social media will be whom they say they are. There can be people who pretend to be someone else and could cause you harm. For example, they may

want to trick you into sharing private or personal information that they could use against you. Once you make a friend online, it doesn't have to be permanent. Regularly review and clean up your contacts.



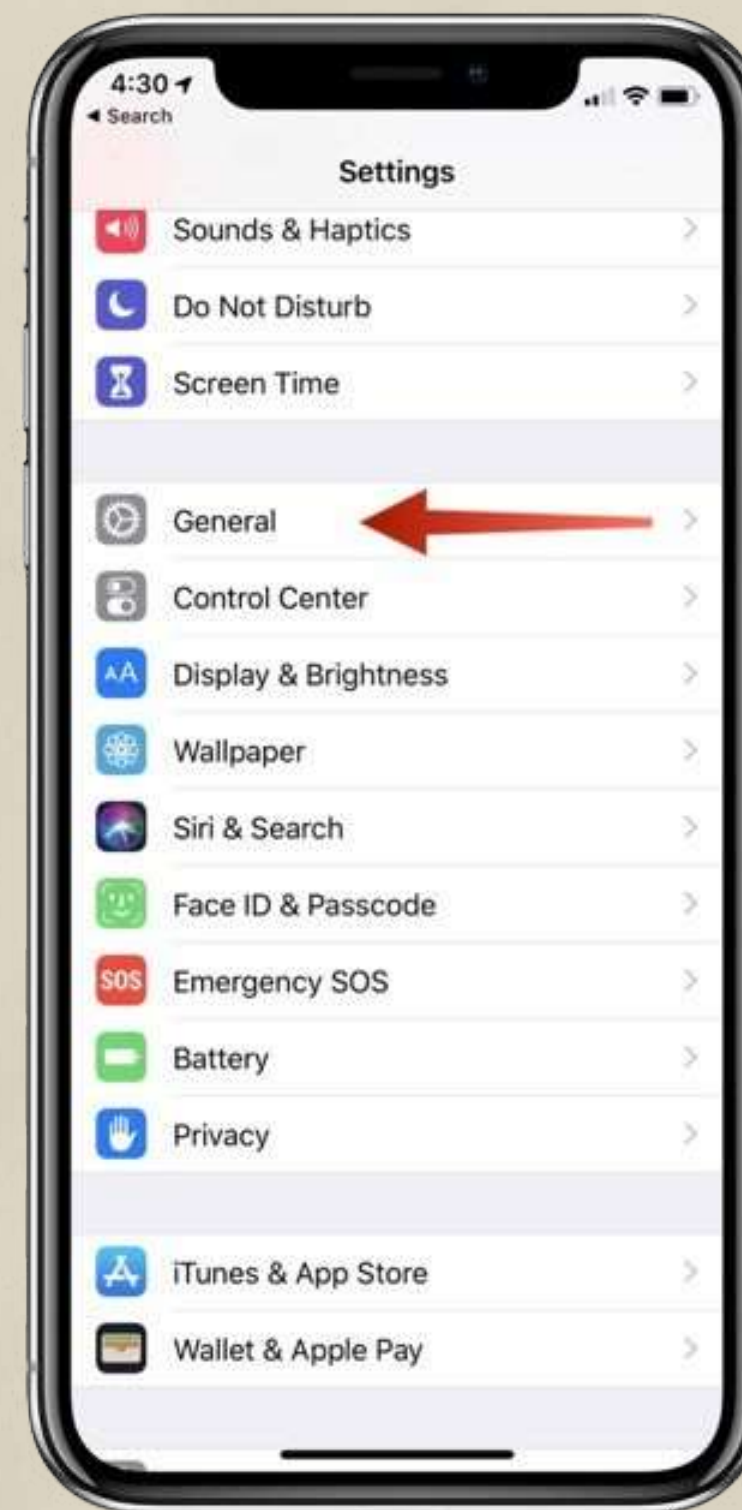


How to manage your digital footprint?



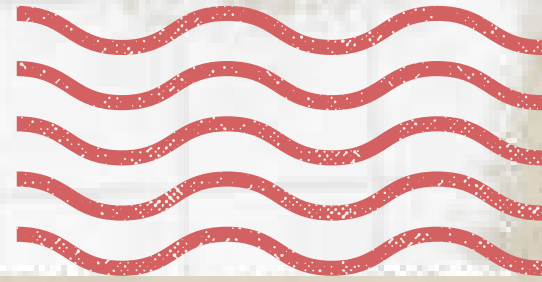
9. Always update your software.

Outdated software can give hackers a backdoor for accessing your private information. Keeping your antivirus and other programs updated means you get security patches that will help fix or remove bugs in your system. You can set programs and apps to auto-update so you're sure you have the latest software installed.



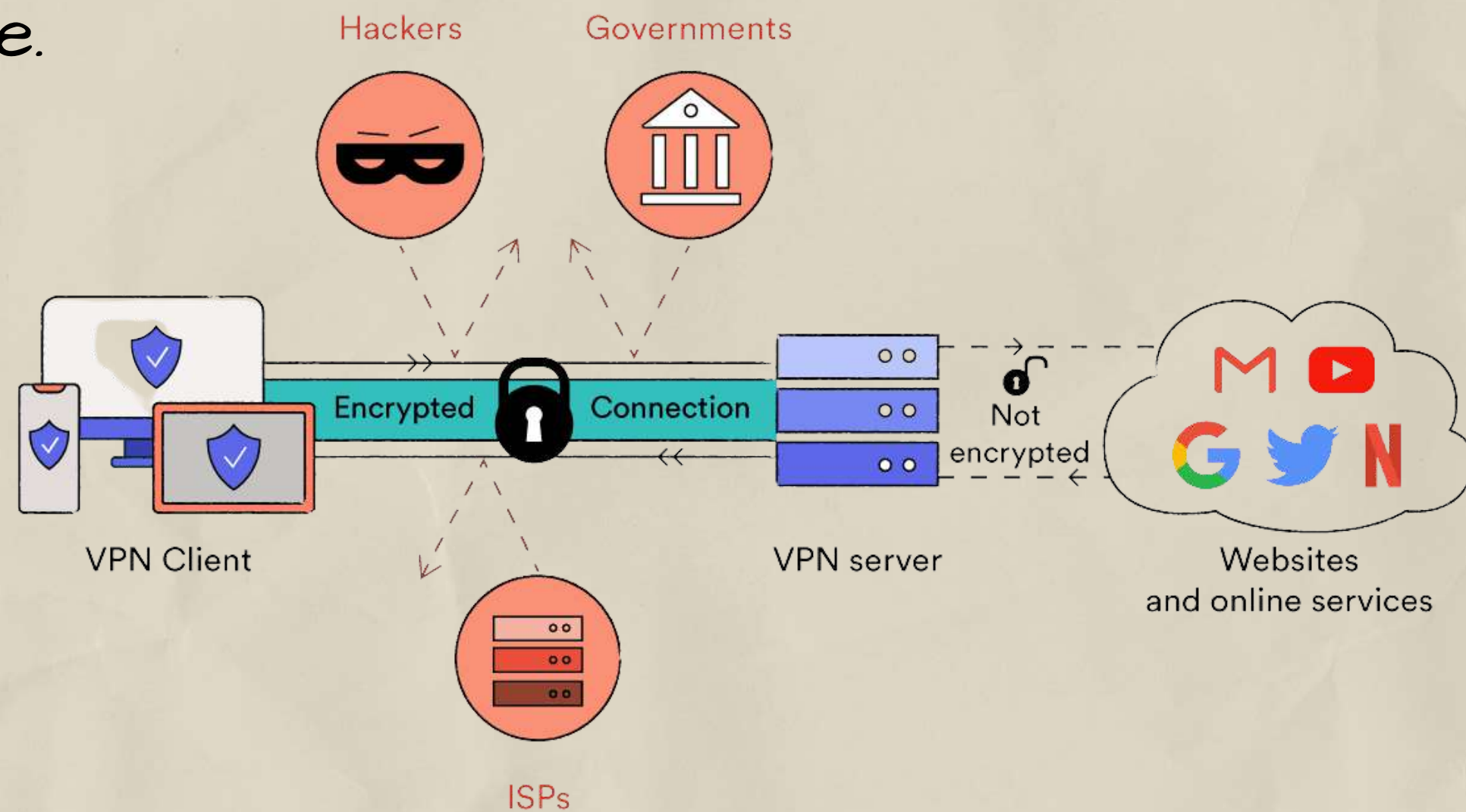


How to manage your digital footprint?



10. Use virtual private network tools.

To protect your privacy, you can use anti-tracking tools, private search engines, or anonymous browsers. Virtual private networks (VPNs), mask your IP address so you can keep your location, browsing history, and other information private.





What does
cyber-bullying
mean?

How to
protect
yourself?

How to
protect
others?



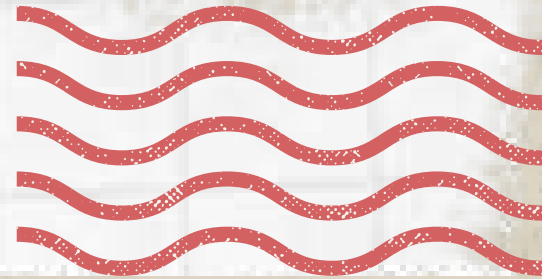
What does cyber-bullying mean?



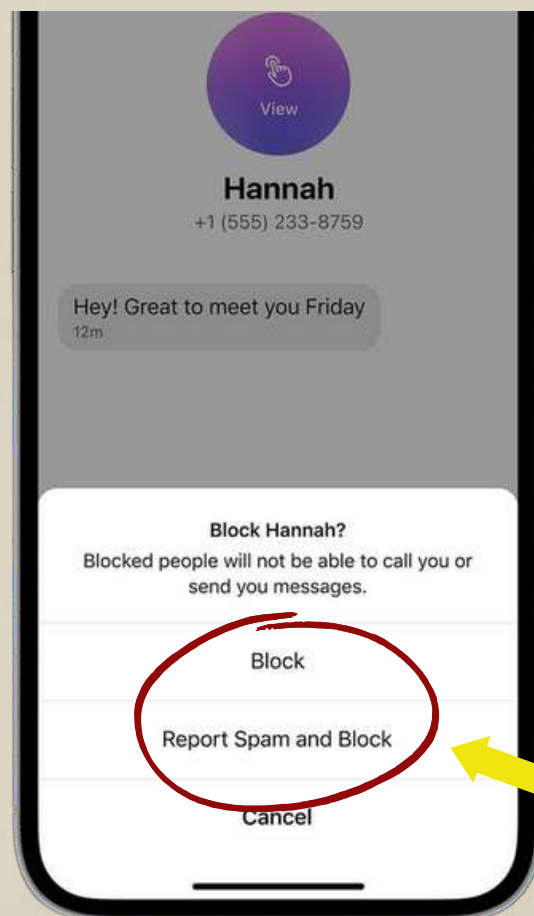
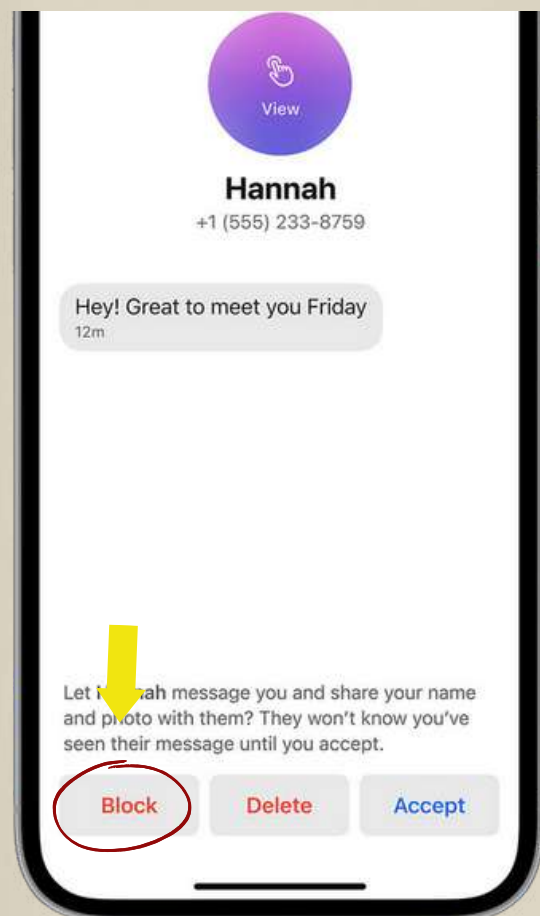
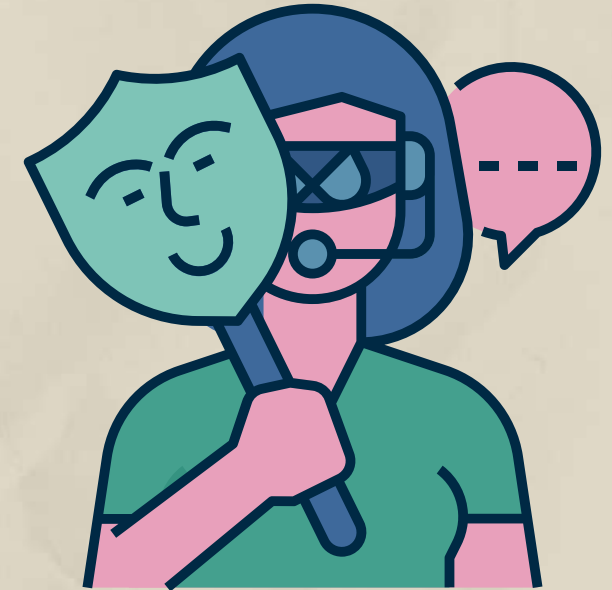
There are many social platforms where people create and share different content. One of the biggest dangers of this is that users often act recklessly due to the need for connection, attention, and recognition. What they wouldn't do otherwise in real life is done much more easily on the internet, with less inhibition. That **misuse of information technologies with the intention to harm others** is called cyber-bullying.



How to prevent cyber-bullying?



Virtual users abuse social platforms to harass their so-called "friends". Sometimes these people are using fake identities and accounts, or resort to anonymizing tools to hide their identity so they could bully others behind virtual masks.

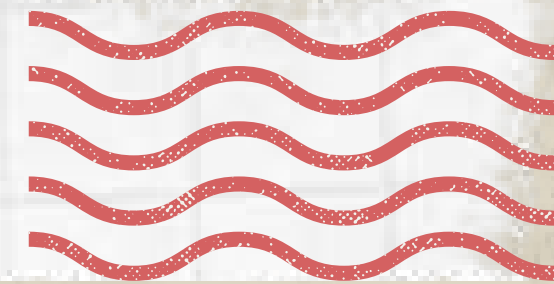


There are 7 simple steps to prevent cyber-bullying:

- Increase your privacy.
- Don't over share.
- Choose not to respond.
- Talk to someone.
- Block the person or people.
- Save the evidence.
- Report to platforms / authorities.



Be aware of the effects of your posts on others



Sometimes people think that what they are doing is harmless or just a joke when they post a video or picture that will make someone embarrassed or share advice about alternative medicine from untrustable resources, etc.

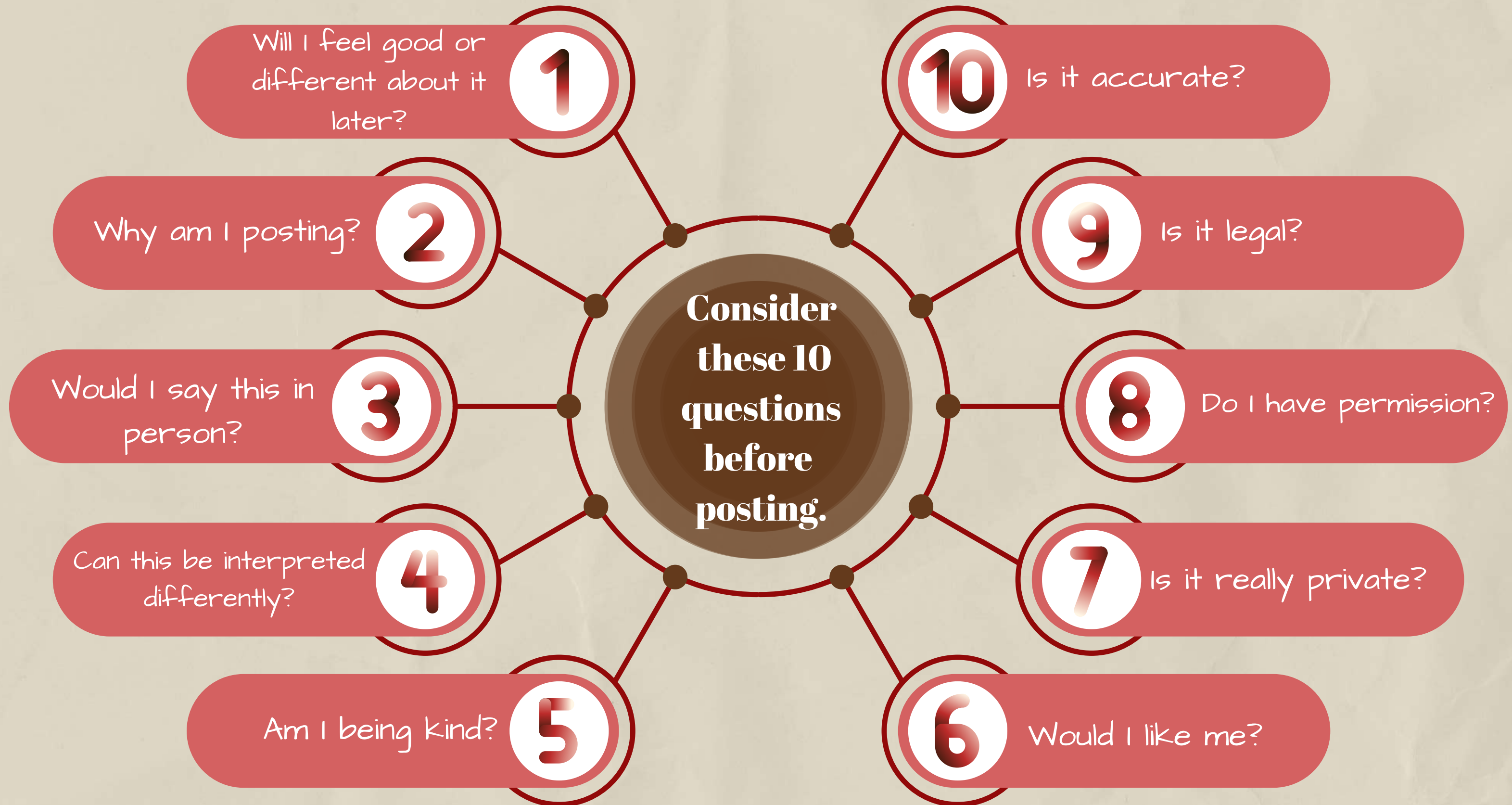
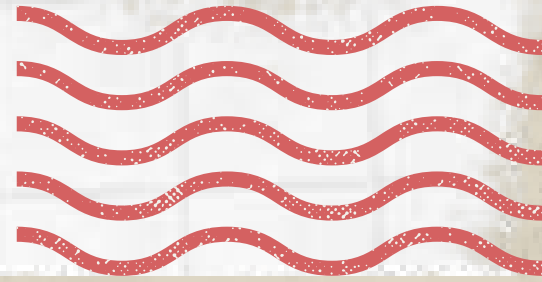
But the truth is the digital world is a real world with real consequences. Once you post, you lose control of the social, traumatic, and psychological effects on an individual of your sharings.



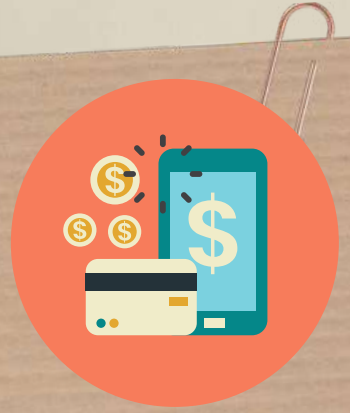
*Don't misuse social networks
to shame and bully others!*



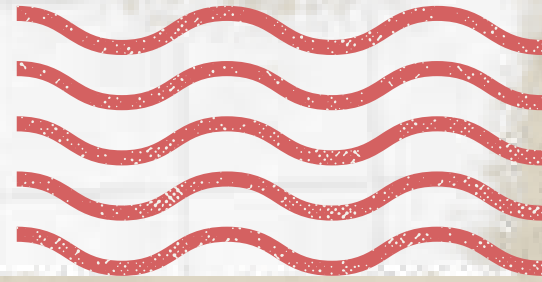
Always ask yourself the following before you hit send!







What is online banking?



Online and mobile banking is a secure way to handle your finances from the comfort of home or you're out and about.

What can I use online banking for?

Check your balance.

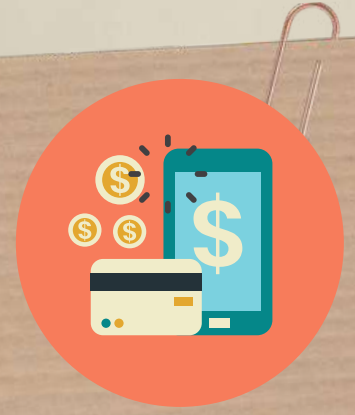
Pay bills

Check your bank statements.

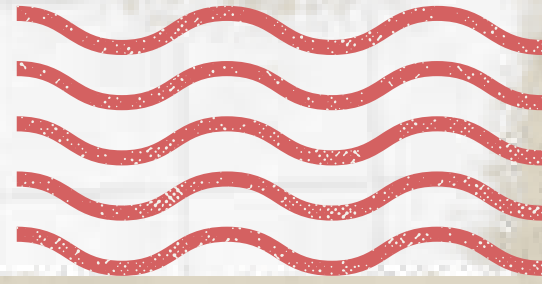
Send money to people.

Transfer money between your bank accounts

Set up or cancel direct debits and standing orders.



How do I set up online banking?



As long as you have a device with access to the Internet and an account with a bank account eligible for online banking, it's easy to get started:



To access online banking, you'll need to register first through your bank's website. Each bank has a slightly different process to set up online banking, and you should speak to your bank.

Steps may include the following:

- Entering your personal and bank account details (sort code and account number).
- The bank may call you and ask you some questions to verify your identity and send an activation code or text.
- Setting up a username and a secure password or passcode.



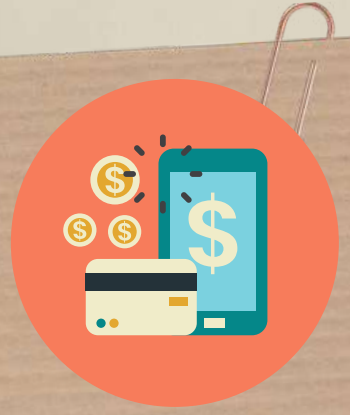


What can I do to keep my money and identity safe?

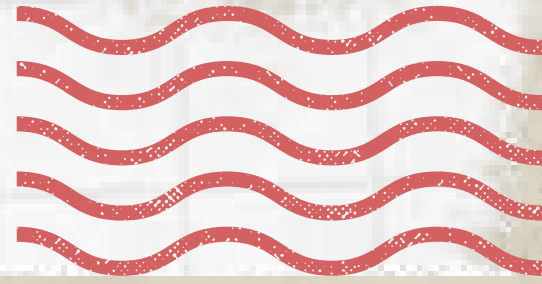
1. Only use secure wifi networks & devices to access your online banking.

If you use public networks, such as those in cafés or train stations, it may be possible for people on the same network to access your details. Also, be cautious when using a public computer to access your online banking. They may not have the right level of security software.





What can I do to keep my money and identity safe?

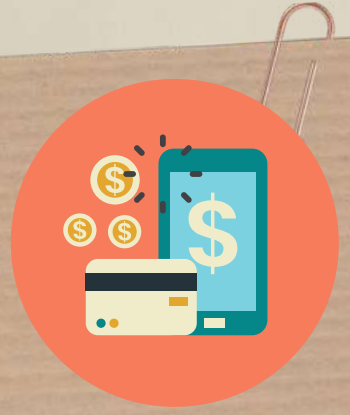


2. Use different login details and passwords for online bank accounts.

Do not use any of the login details you use for online banking for any other online portals or services. Make sure to create a strong password and change it regularly.

3. Do not give your online banking login details to anyone.

Keep them to yourself, just like any pin codes and other sensitive authentication information.

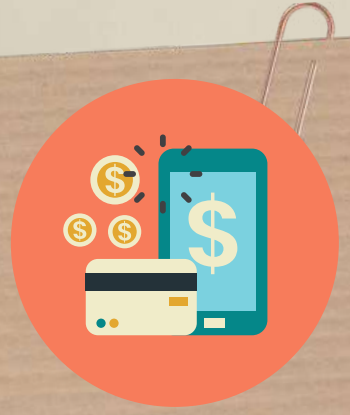


What can I do to keep my money and identity safe?

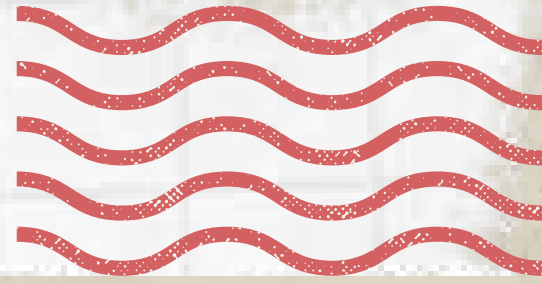
4. Be aware to whom you transfer money.



Only transfer money to parties you trust. A money transfer can usually not be undone without the explicit permission of the receiving party.



What can I do to keep my money and identity safe?



5. Use identity theft-protection software or a VPN.

Consider downloading identity theft-protection software. It is a service that encrypts your internet connection to keep it safe. These services can often come with several protective measures packaged into one, including a VPN and password monitoring.

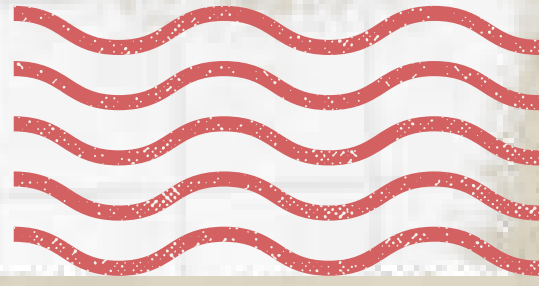


Shopping safely online

Online shopping can make life much easier and takes the hassle out of going to the supermarket or shopping center. You can shop online from most supermarkets, high street shops, as well as smaller independent shops.

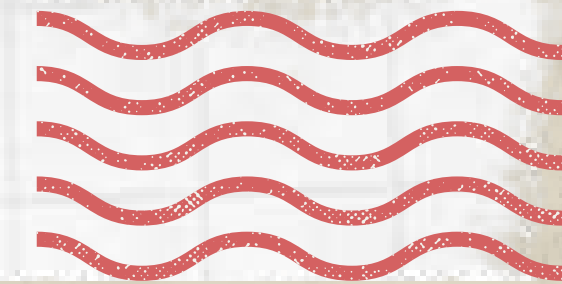
Goods can be delivered directly to your house, usually for a small fee or for free, or you can also use a service called 'click and collect' where you order online but collect items in-store.

But it's important to use safe and genuine websites. Here are a few tips for protecting your money and personal information when shopping online.





Shopping safely online

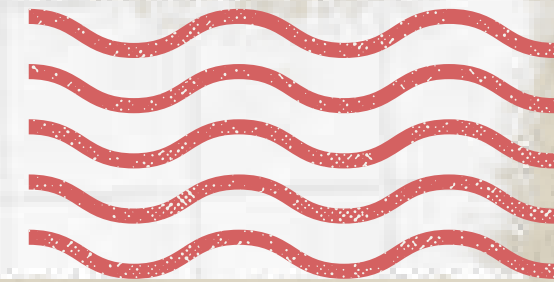


Tip 1: Choose the website that you are shopping carefully and shop with reputable retailers.



Use online retailers with a good reputation, such as well-known supermarkets, high street shops, or established online stores. Look for the company's full contact details. A reputable company will always display this information on its website. Search for the name of the company on the internet to see if anyone has experienced problems with the retailer.

Shopping safely online

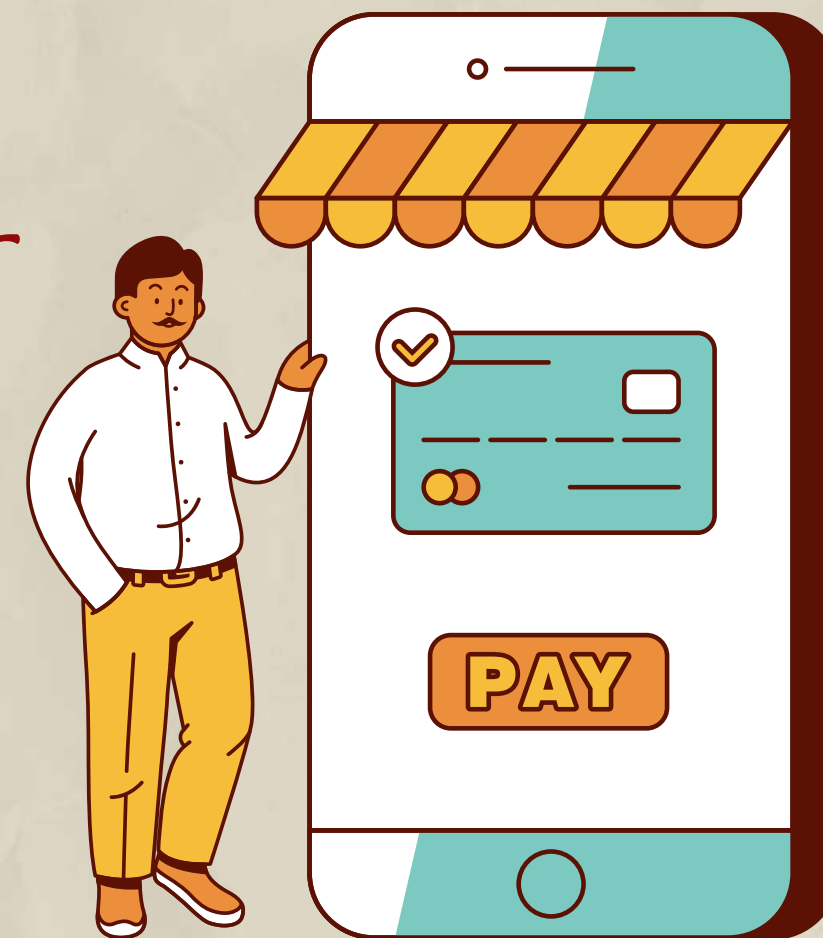


Tip 2: Use the same card for internet transactions only.

Check the bank statement for this card regularly for any unusual transactions and contact your bank immediately if there's a problem.

Tip 3: Use a credit card, rather than a debit card, for internet transactions.

It will provide additional protection. If your purchase costs more than 100 GBP and you use a credit card, the seller and your card company are equally responsible if anything goes wrong.



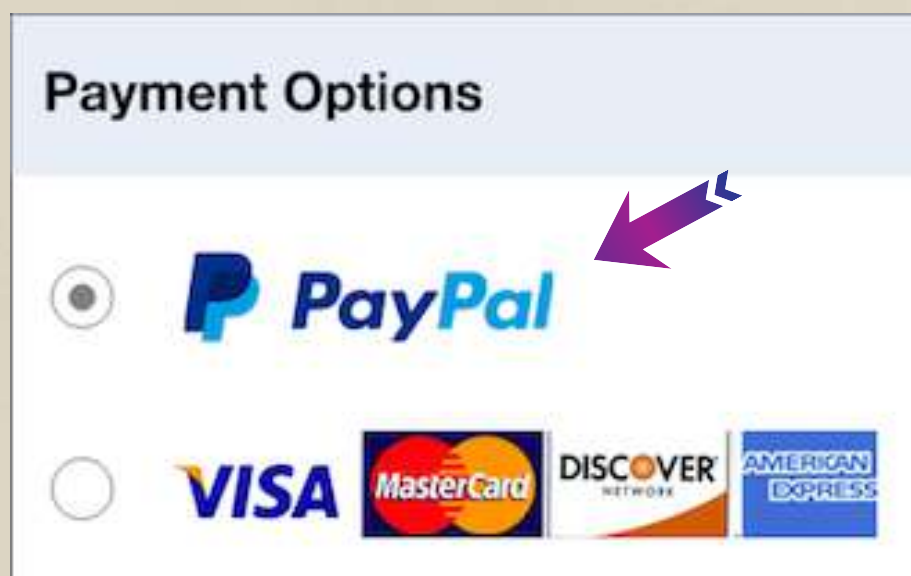


Shopping safely online

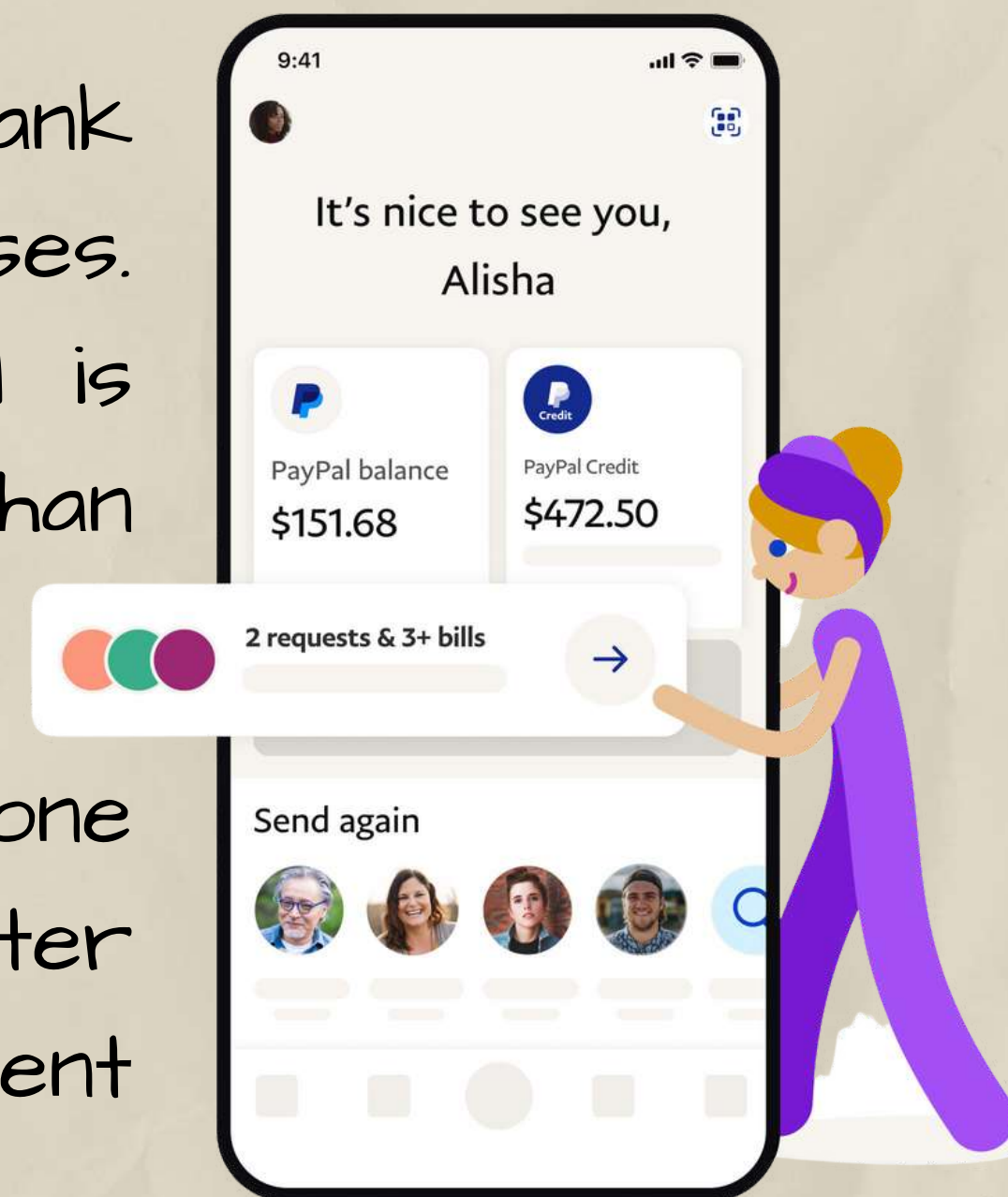


Tip 4. Consider using a PayPal account.

This is an online account that you link to your bank account or payment card to pay for online purchases. If you don't want to use a credit card, PayPal is secure and comes with more payment protection than a debit card.

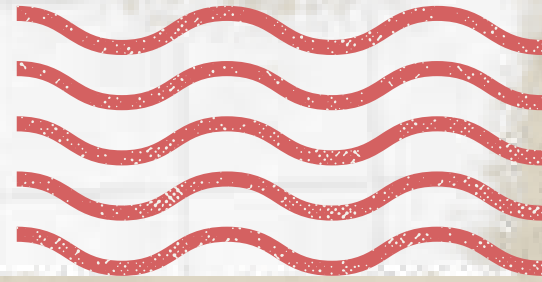


Download the app on your phone or sign up for free online. After that, you can use it as a payment option for your purchases.



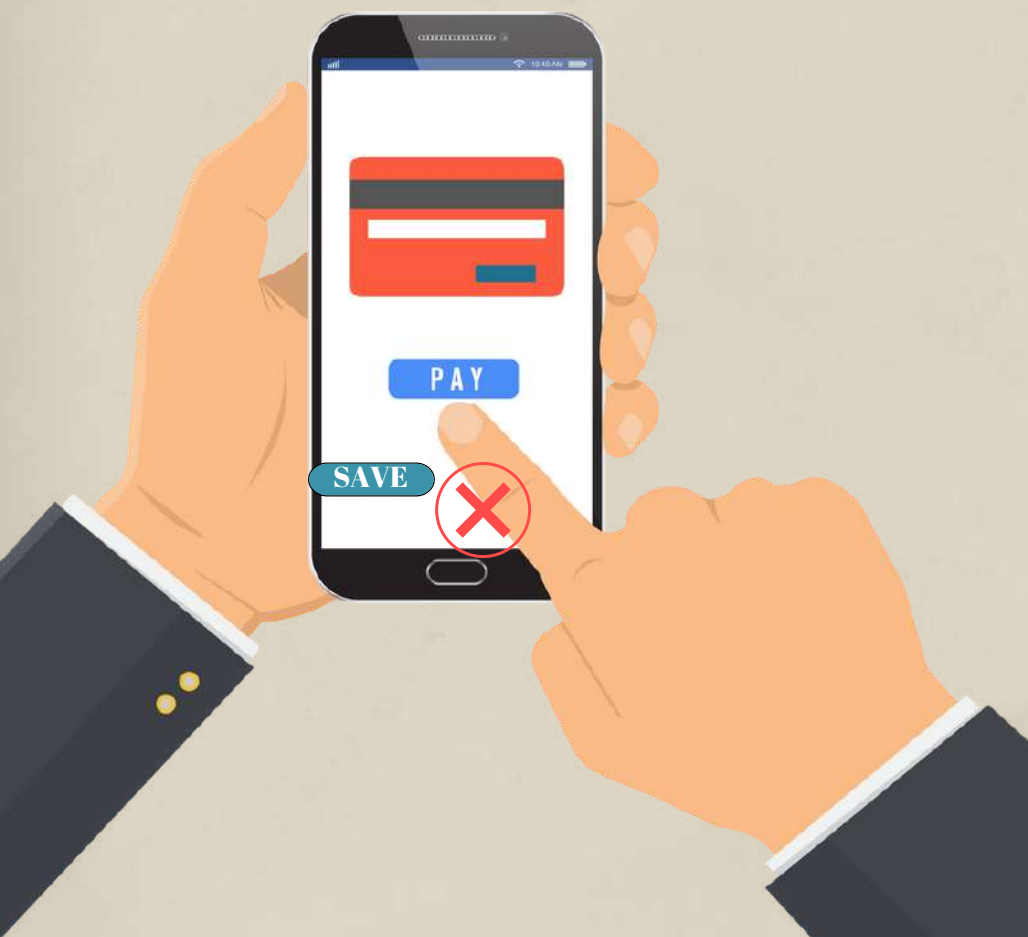
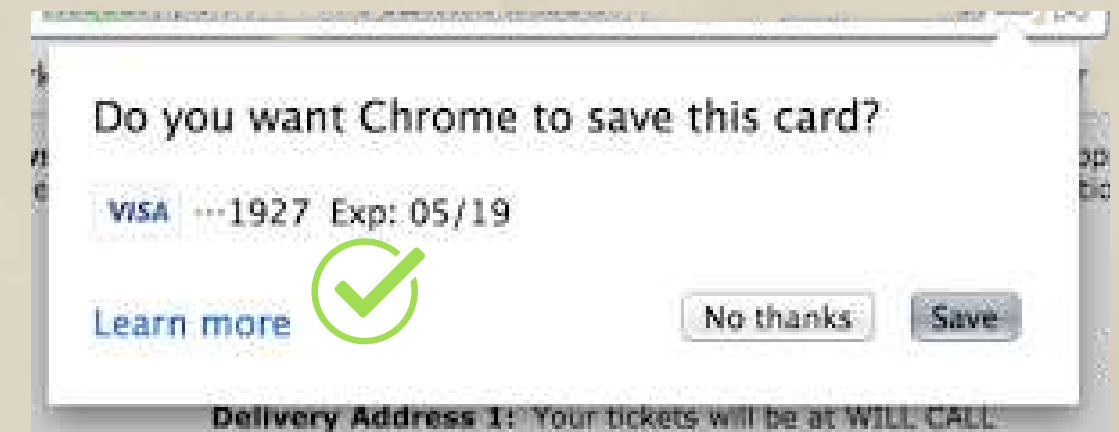


Shopping safely online



Tip 5. Don't save your card details.

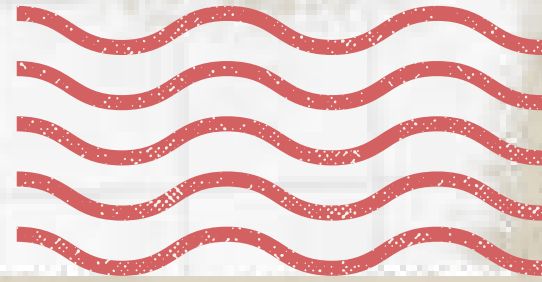
Sometimes the website or your internet browser prompts you to save your card details for next time.



Never do this on a shared computer, and make sure your device is protected with a password, PIN or fingerprint log in if you do save your card details.



Shopping safely online

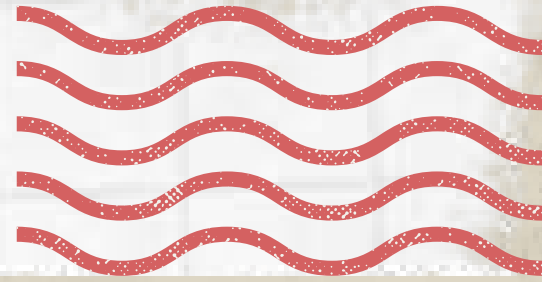


6. Don't fall for email scams

You might get emails or texts offering amazing bargains or claiming there's been a problem with a package delivery. Delete suspicious messages from unfamiliar senders. And don't open attachments or click links in messages because they could infect your computer or phone with viruses and other malware.



Shopping safely online

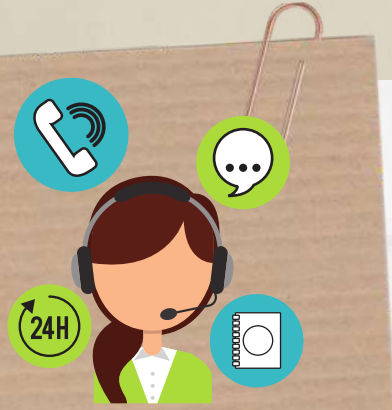


7. Track your delivery.

After you make an online purchase, keep tabs on it to make sure it's headed your way. If the merchant refuses to provide shipping info or respond to your requests for the status of your order, contact your credit card issuer for help. They may remove the charge from your bill and look into the matter.



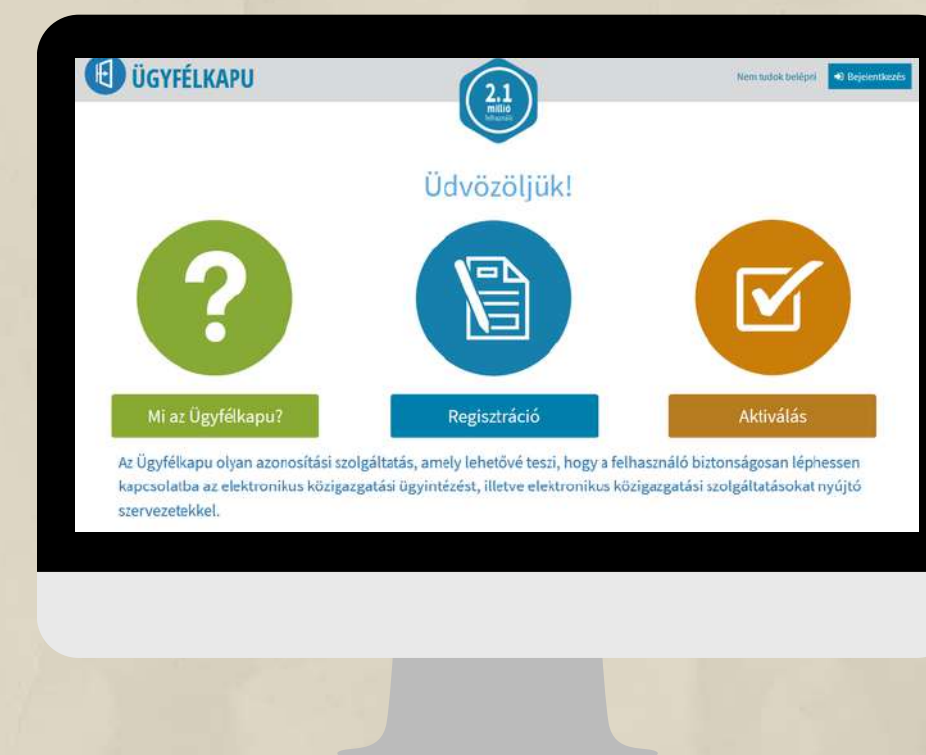




Ügyfélkapu (Client Gate Portal)



Ügyfélkapu is the electronic identification and customer access system used by the Hungarian government. It ensures that its users can safely contact the bodies providing electronic public administration services with a single login, in addition to giving proof of identity. As a result, you can manage administrations with it quite effortlessly and fast.

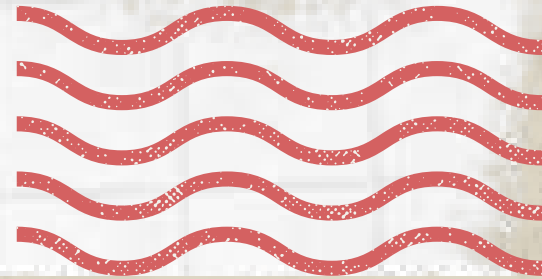


Who Can Have a Client Gate account?

Anyone can use it. More specifically, every natural person, regardless of nationality, can register on the Client Gate.



What can be managed through the Client Gate?



The portal allows you to manage a number of things. Here are a few examples of commonly used services:

- you can check whether you are registered at your workplace
- you can apply for maternity allowance, GYES, family allowance
- you can ask for a moral certificate
- you can do your self-declaration
- you can query your current tax account from NAV



The comprehensive list is available here:

<https://ugyintezes.magyarorszag.hu/szolgaltatasok?selected=A>





Where can it be set up?

- In any document office,
- In the government office (you can book an appointment online),
- At the main customer services of the Tax Authority (NAV) (you can book an appointment online),
- At some postal customer services (in small towns) or
- Electronically.

What steps are necessary to launch a customer portal?

1. Official identity card suitable for personal identification
2. Unique username
3. Email address

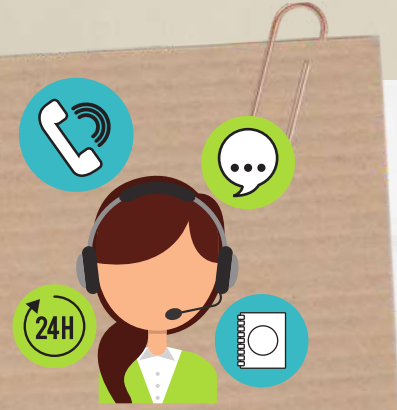
LOGIN

Username

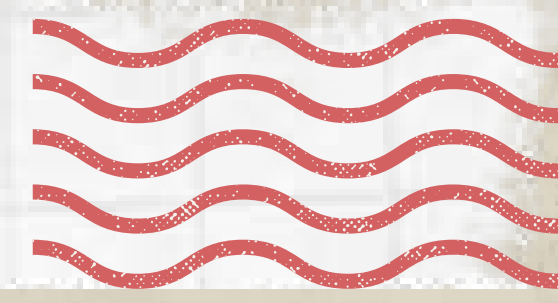
Password

SIGN IN

Remember me [Forgot your password?](#)



How to Create an account on Client Gate?

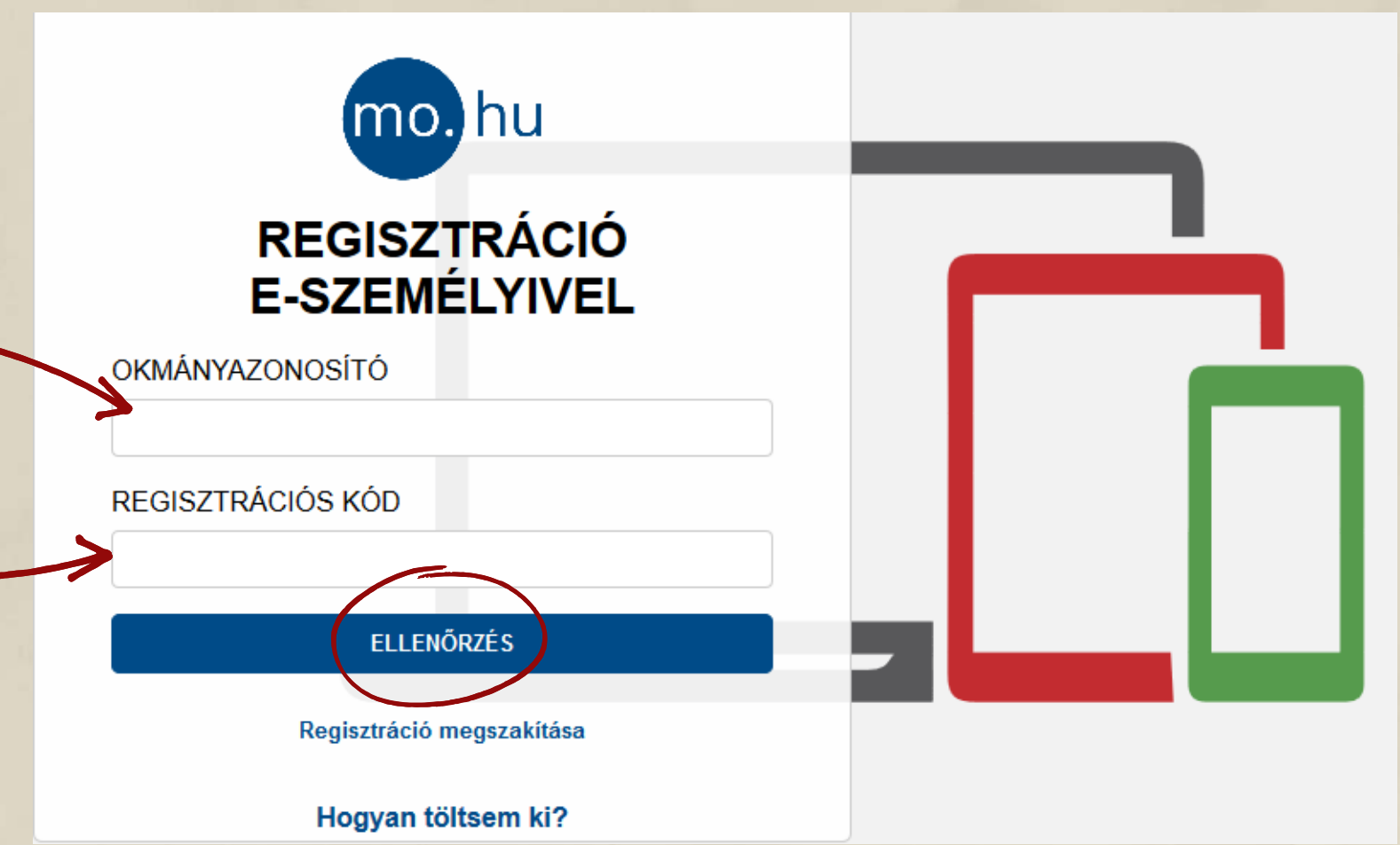


Go to <https://ugyfelkapu.gov.hu/regisztracio> to register. Here, click the "E-PERSONAL" button. The form "REGISTER WITH E-PERSON" appears.:

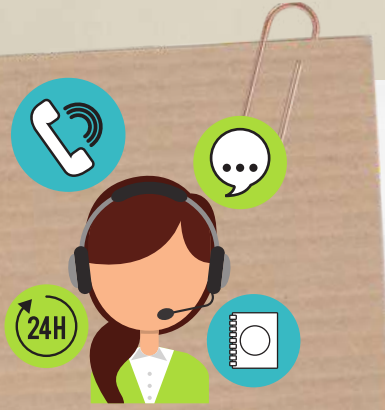


The **document ID** is the 6-digit and 2-letter ID that appears on your e-ID.

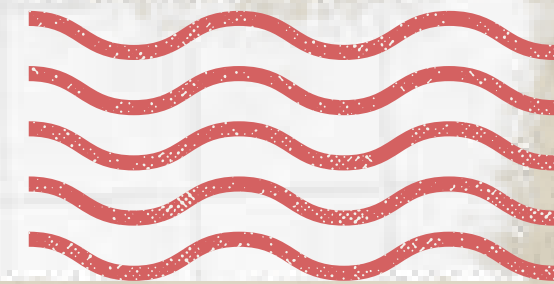
The **registration code** is a sequence of 11 digits and letters that you received in a sealed envelope when you applied for your personal identity card.



After inputting the data, click the "CHECK" button.



How to Create an account on Client Gate?



The form will be filled out with your information. Scroll down and enter the following:

The username: Must be unique for each user. If the username you pick is already used, you should choose another one.

In the "**Confirm email address**" area, the same e-mail address must be typed.

ÜGYFÉLKAPU REGISZTRÁCIÓS ADATAI

Felhasználónév

Email cím

Email cím megerősítése

ELŐZETES ÉRTESÍTÉST KÉREK OKMÁNYAIM LEJÁRATÁRÓL

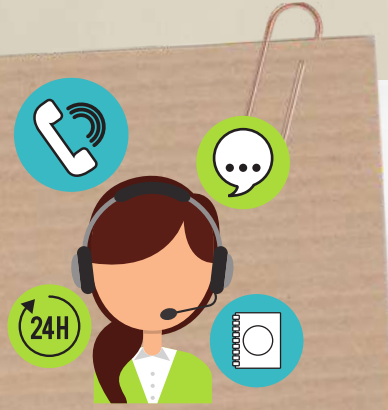
IGEN

REGISZTRÁCIÓ

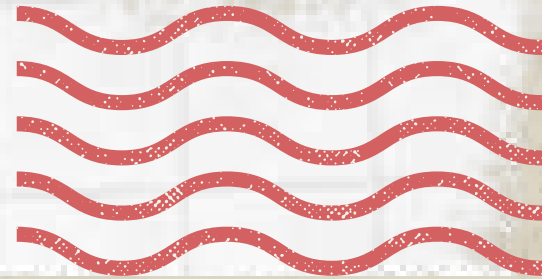
Your one-time activation code for the initial login will be emailed to you at this address.

"I request prior notification of the expiration of my documents" field is checked by default. The service is free for all customers with a Client Gate registration.

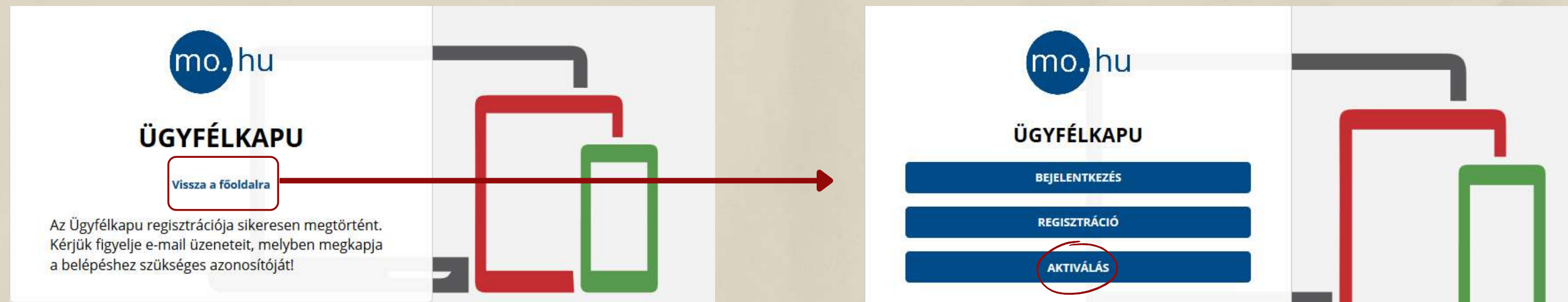
If you have completed all of the fields, click the "Register" button.



How to Create an account on Client Gate?

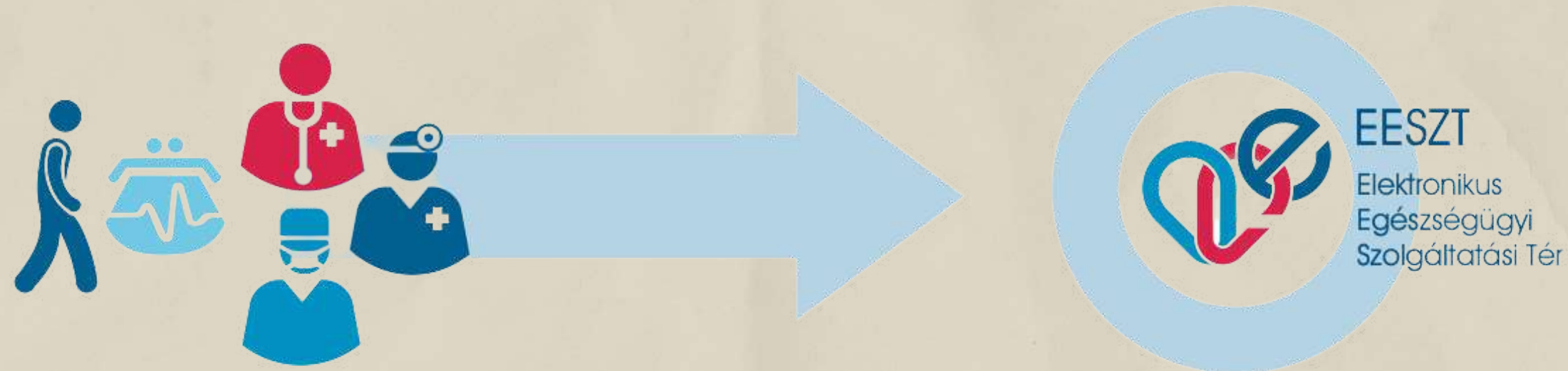
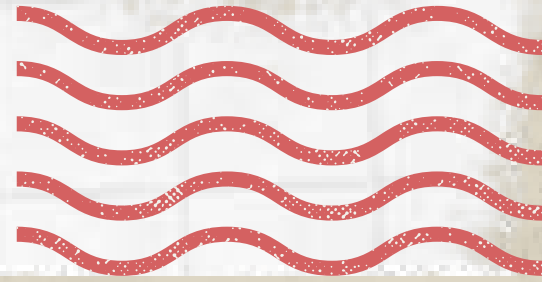
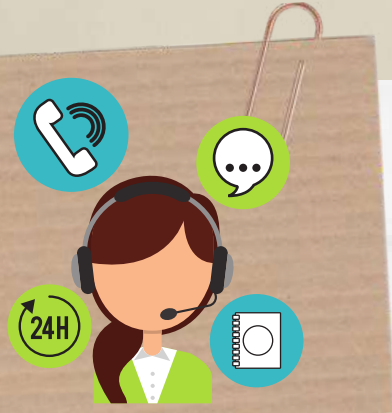


You will receive information about the success of the registration in a message window. If you click on the text "Back to the main page", the following will appear on the screen:

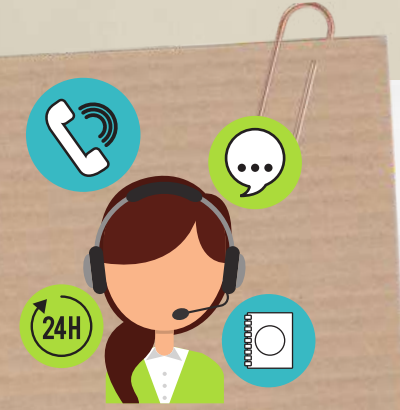


Select the "Activate" button. You must create a password that is at least 8 characters long and includes at least two digits as well as a mix of upper and lower case letters. The password is valid for two years and must be changed after then.

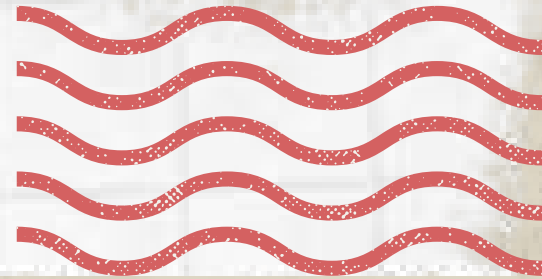
The Electronic Healthcare Service



The Electronic Health Service, EESZT for short, is the IT system and database connecting health service processes, which enables the implementation of the laws requiring the compulsory collection of data for those provided in the Hungarian health care system. In addition to personal data, the EESZT database is used to collect, store and share findings, prescriptions, and information related to various medical examinations for the duration of the patient's life (and five years after that).

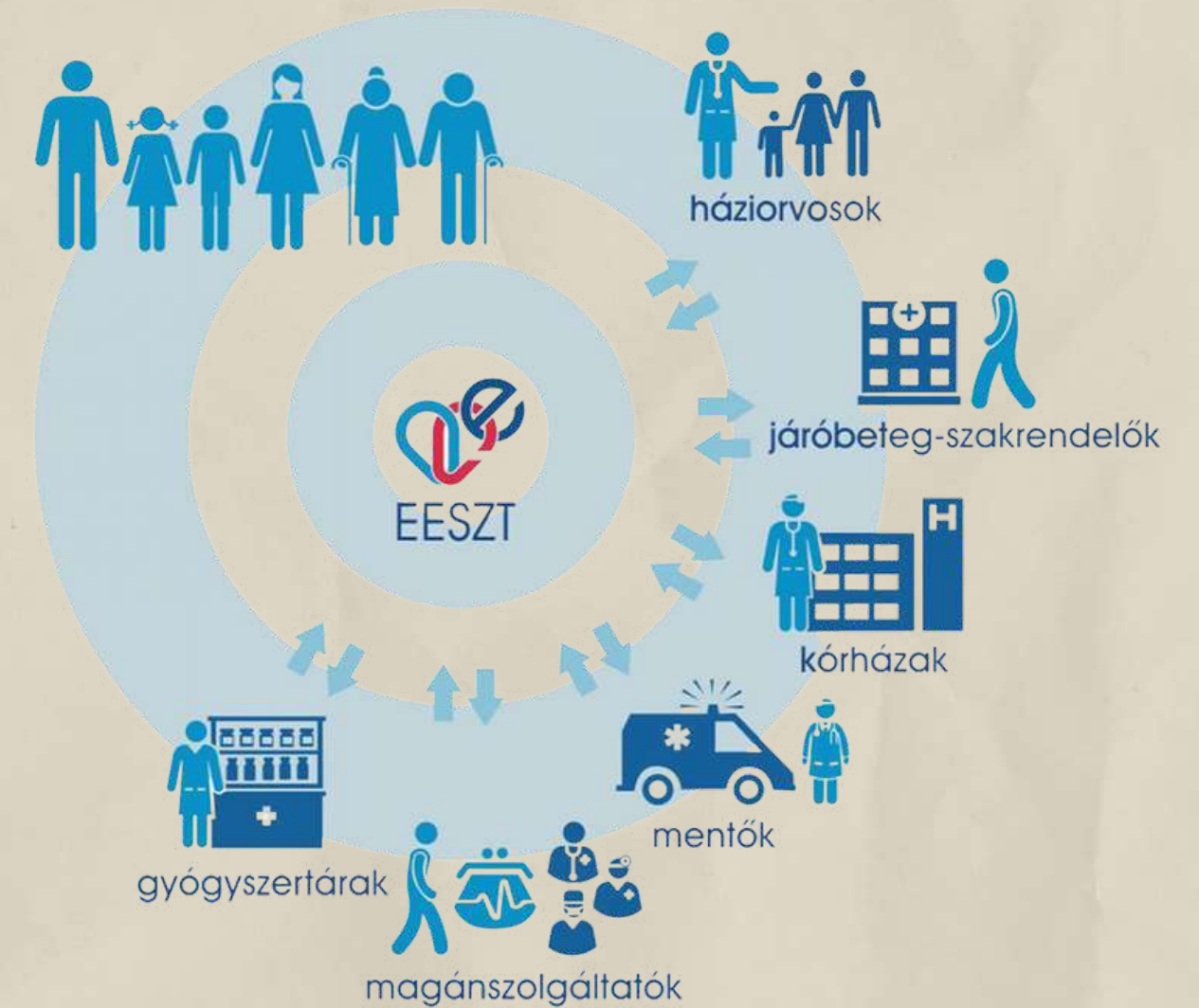


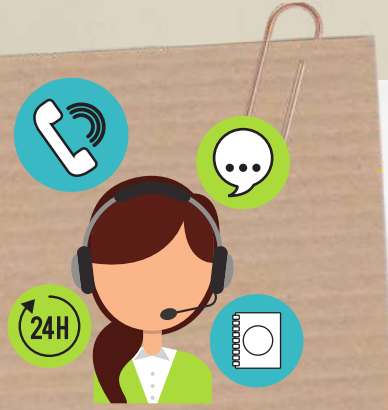
The Electronic Healthcare Service



Prescriptions, recommendations, outpatient data, laboratory findings, X-ray, CT, and MR findings, and final reports are all available on the portal online. These publications can also be downloaded in pdf format and saved on a computer before being printed.

The e-Recipes appear in the list as well, with a clear distinction between those that have already been activated and those that are still awaiting activation. Since December 31, 2019, prescription certificates uploaded to the system by the patient's doctor have replaced the regular prescription. Service users can find e-Recipes in pharmacies by providing their TAJ number.





Entry into the EESZT system as a residential customer



EESZT
Elektronikus Egészségügyi Szolgáltatási Tér

FŐOLDAL NYILVÁNOS KÖZTÉRZSEK

BEJELENTKÉZÉS ?

Állampolgári bejelentkezés

- 1 Bejelentkezés
- 2 TAJ autorizáció
- 3 Sikeres bejelentkezés

Az Ügyfélkapu bejelentkezési ikon megnyomásakor átkerül az Ügyfélkapura, ahol az ügyfélkapus azonosítóival kell belépnie. Amennyiben néhány percen belül már volt sikeres ügyfélkapus belépése, előfordulhat, hogy nem kell megismételni a belépést, hanem automatikusan beléptetésre kerül az ügyfélkapun és a 2. folyamatképernyőre kerül átirányításra!

ÜGYFÉLKAPU BEJELENTKÉZÉS

Fenntartó Adatvédelem Impresszum
+36 1 920 1050 helpdesk.eeszt@aek.hu

Az EESZT adatkezelését a NAIH auditálta

SZÉCHENYI 2020
Magyar Nemzeti Elektronikus Egészségügyi Szolgáltatási Tér
EUROPEAN UNION
EUROPEAN REGIONAL DEVELOPMENT FUND
BEFEKTETÉS ÉS JÖVŐ

Állami Egészségügyi Ellátó Központ © 2015 - Minden jog fenntartva

Patients access the EESZT system by entering the Client Gate. The TAJ number must be entered after opening the portal in order to access the EESZT system.

Where and how can it be used?



At the family doctor's office:

Your family doctor discovered in the e-Prescription system that the patient failed to switch one of his critical heart drugs. Due to the patient's deteriorating health, he collected blood for laboratory tests and sent him to a cardiologist specialist.

At the specialist appointment: The cardiology specialist appointment also took into account the detailed data of the e-referral, the patient received a diuretic injection, which improved the short observation, and based on the blood test results visible through the EESZT, his medications were changed, and prescriptions were also written to him in the e-Prescription system.

At the pharmacy: The patient went to the nearest pharmacy on his way home, where he received the prescribed medicines by presenting his e-Personal ID card (or TAJ card and identity document).

At home: In the evening, out of curiosity, Mr. Kovács accessed the Citizens' Portal, reviewed the occurrences of the day, and verified that both his care and data management met his expectations.

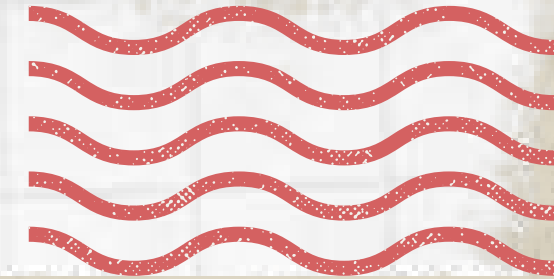
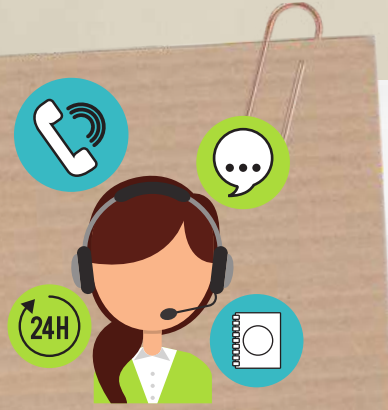
At home: Mr. Kovács has been experiencing increasing leg swelling and suffocation for several days, so he consulted to the family doctor.

Family doctor - the next day:

At the beginning of his next day's appointment, Mr. Kovács' family doctor looked up the previous day's events. From the EESZT, his family doctor program displayed the specialist's opinion, and he was also able to make sure that Mr. Kovács had not forgotten to replace his medication.



The KRÉTA Electronic Diary



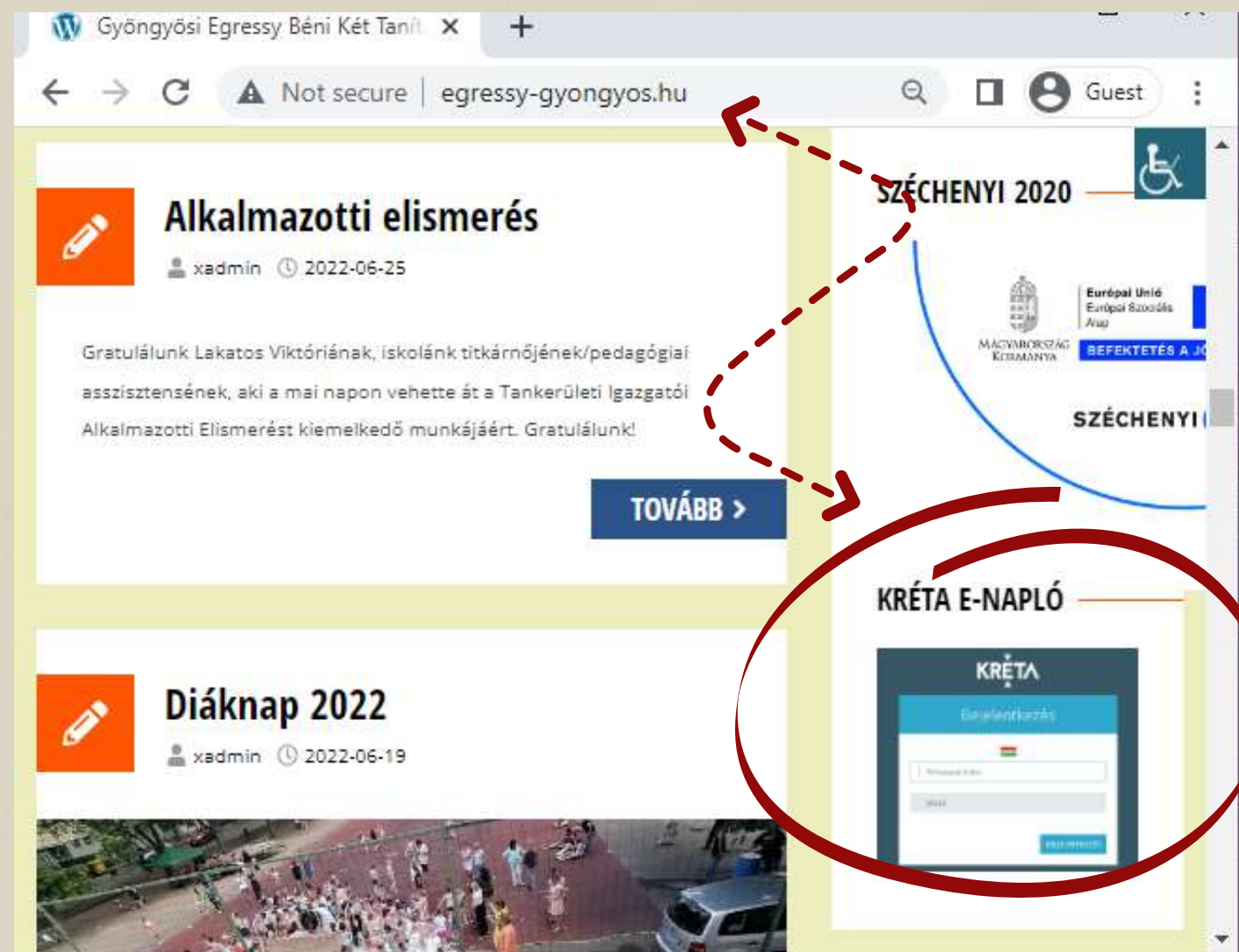
The KRÉTA Electronic Diary helps parents and students access up-to-date information during their studies on a desktop computer, via any browser program.

The e-Diary makes study data accessible from any location. Students and parents can usually access it by entering the web address of their own institutional system.



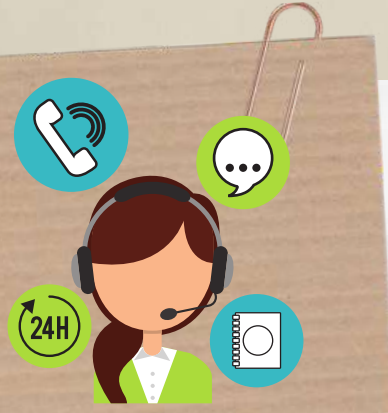
How to Enter the Kréta?

After entering the school's webpage, look for the KRÉTA link on the school's homepage.

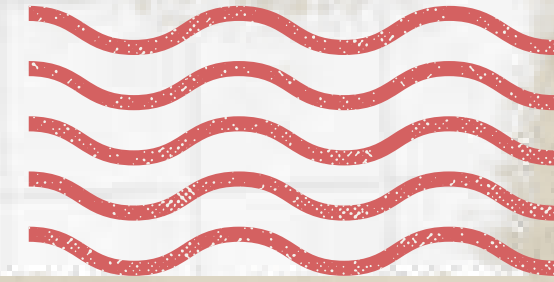


Logging in is possible using the students' OM ID (which varies for each student; please inquire at the school) and the date of birth as a password, separated by a hyphen (for example: 2010-01-01).

Each school has a different KRÉTA page, you can only enter on the school's own KRÉTA page!

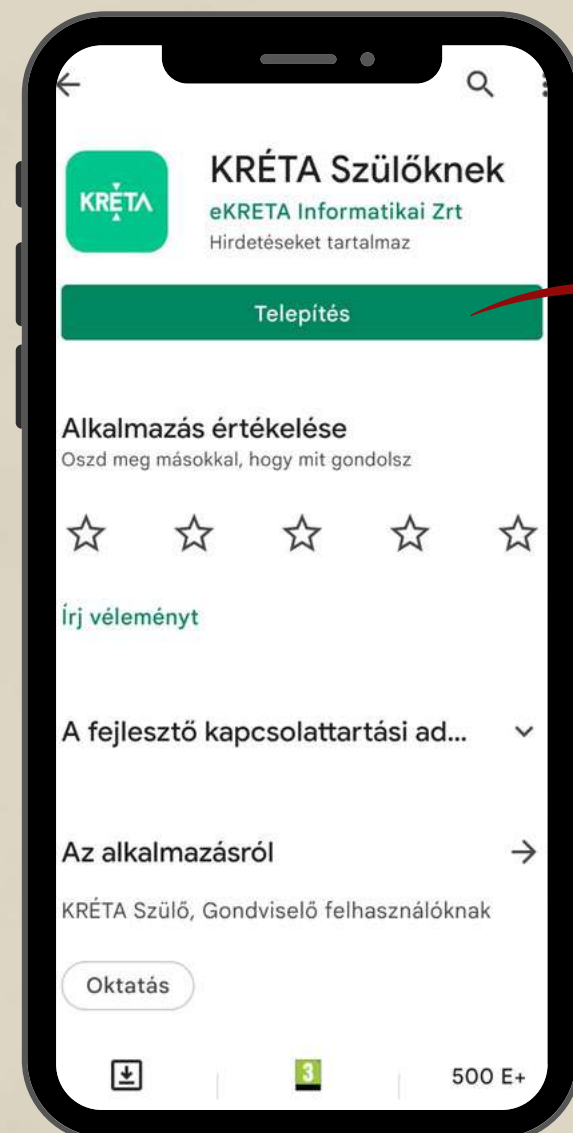


Using the Kréta Electronic Diary on a mobile phone



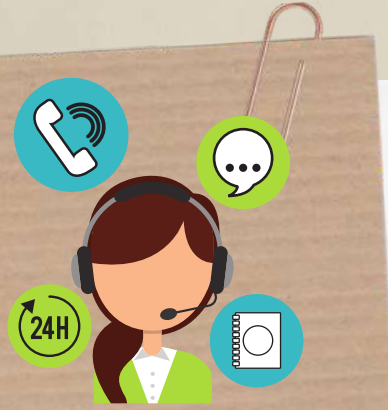
The KRÉTA Mobile applications available for Android, iOS and Huawei devices provide useful assistance to students and parents of institutions that use the KRÉTA e-diary.

The system provides assistance in the effective monitoring of students' academic progress and the related administration.

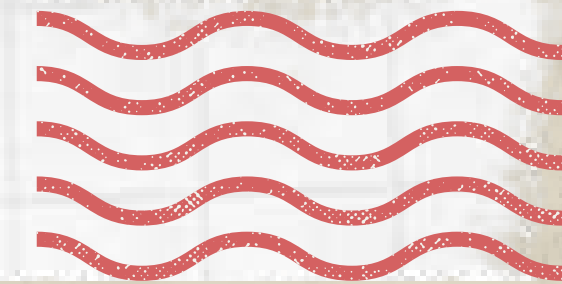


Download the application. After downloading, launch the program and install from there.

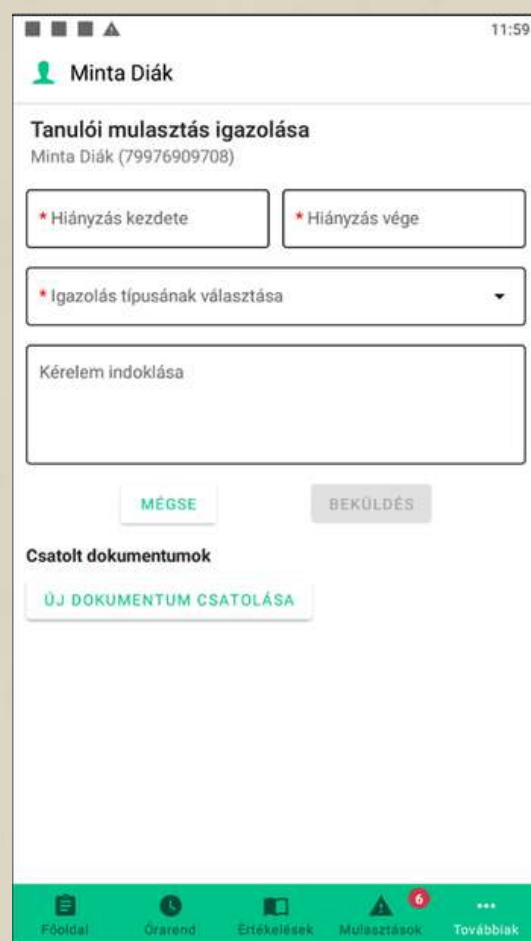
You must enter the KRÉTA mobile application with the same student or parent username and password as on the web interface.



Using the Kréta Electronic Diary on a mobile phone



The app allows users to view student schedules, reported assessments, homework, absences, and other student-related information.



The data needed for administration are managed by the student's institution.



STAY SAFE ON SOCIAL MEDIA

<https://safety.google/security/security-tips/>

<https://us.norton.com/internetsecurity-privacy-password-security.html>

<https://www.kidscape.org.uk/advice/advice-for-young-people/dealing-with-cyberbullying/staying-safe-on-social-media/>

<https://www.facebook.com/help/122006714548814>

DATA PROTECTION & DIGITAL FOOTPRINT

<https://www.gov.uk/data-protection>

<https://www.familylives.org.uk/advice/your-family/online-safety/digital-footprints>

<https://www.security.org/digital-safety/>

<https://staysafeonline.org/online-safety-privacy-basics/5-ways-spot-phishing-emails/>

R
E
F
E
R
E
N
C
E
S

CYBER-BULLYING

https://www.researchgate.net/publication/358402280_Bullying_Cyberbullying_and_Hate_Speech

<https://www.unicef.org/end-violence/how-to-stop-cyberbullying>

<https://www.kidscape.org.uk/advice/advice-for-young-people/dealing-with-cyberbullying/think-before-you-post/>

<https://www.brandwatch.com/reports/cyberbullying-2016/>

ONLINE BANKING & SHOPPING

<https://www.ageuk.org.uk/globalassets/age-uk/documents/digital-instruction-guides/a-beginners-guide-to-staying-safe-online.pdf>

<https://www.consumerfinance.gov/about-us/blog/online-mobile-banking-tips-beginners/>

<https://www.safewise.com/blog/10-cybersecurity-tips-for-online-shopping/>

R
E
f
E
R
E
N
C
E
S

ONLINE ACCESS TO PUBLIC SERVICES

<https://www.bdo.hu/hu-hu/aktualitasok-blog/miert-erdemes-a-maganszemelyeknek-ugyfelkaput-nyitniuk>

<https://regi.ugyfelkapu.magyarorszag.hu/>

<https://www.billingo.hu/blog/olvas/ugyfelkapu>

https://edinaszamol.blog.hu/2019/08/12/hogyan_nyissak_ugyfelkaput

<https://e-egeszsegugy.gov.hu/web/eeszt-information-portal/home>

<https://www.e-kreta.hu>

<https://play.google.com/store/apps/details?id=hu.ekreta.guardian&hl=en&gl=US>

R
E
T
E
R
E
N
C
E
S

SCAN ME



Project "DIGITALIZE - tools for Roma adults to use the internet and promote education"

FOLLOW US!

SCAN ME



SCAN ME



SCAN ME



Amaro
Foro e.V.

facebook.com/AmaroForo/
instagram.com/amaro_foro/



EGYÜTT
HATÓ

KÖZÖSSÉGÉPÍTŐ EGYESÜLET

facebook.com/EgyuttHato/
instagram.com/egyutthato/



NEVO
PARUDIMOS

facebook.com/NevoParudimos/
instagram.com/nevoparudimos/



facebook.com/rromassn.org/
instagram.com/rromassn/

0110G463544