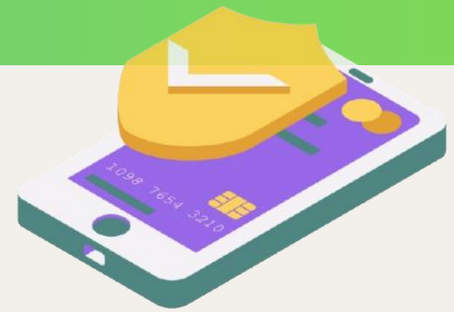
FinaLY
Empowering Financial Literacy in Youth

Digital & Online Financial Behaviour



Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.
Project Number: 2023-3-CY02-KA210-YOU-000185401

Co-funded by the European Union

Funded by:

Co-funded by the European Union

Consortium

FinaLY

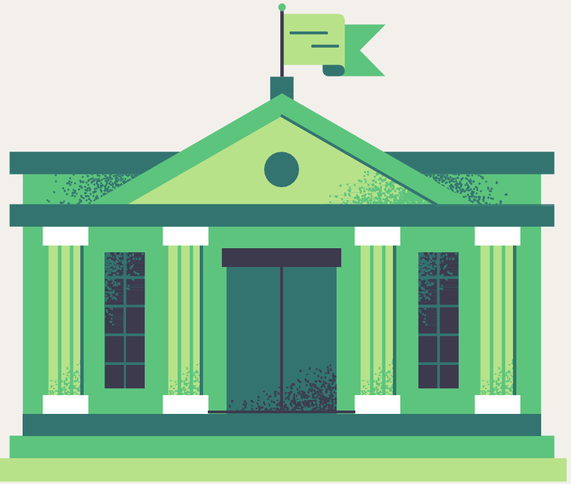
ECECT

comhairle chontae na mí
meath county council

YouthNet Cyprus

Introduction

- The goal of FinaLY is to make young people smarter with financial decisions
- Young adults begin making key money choices like saving and spending, in a financial world full of risks and opportunities
- Many young adults in Europe don’t fully understand basic financial topics like saving, budgeting, or using credit
- According to an international study by the OECD in 2020, about half of EU adults struggle with financial knowledge



Co-funded by
the European Union

Objectives

By the end of this presentation, we will be able to:

- Identify safe websites and payment methods
- Create and manage strong passwords
- Recognize and avoid online scams and phishing attempts
- Use digital wallets (PayPal, Revolut, Apple Pay, Google Pay) safely
- Understand and protect personal data privacy
- Be aware of financial regulations and safety nets.

Co-funded by
the European Union

Welcome to the Digital Money World

We live in a time where money moves with just a **click!**
From online shopping to mobile banking, we **buy**, **save**, and **send** money digitally every day.

But with convenience comes responsibility!
So, let’s learn how to stay:

- **smart**
- **safe**
- **in control**

when using money online.

Co-funded by
the European Union

Why this matters

Your entire financial life can be managed from your phone.

- **One bad click = lost money**

  Accidentally tapping on a fake link or entering your details on the wrong site can drain your account.

- **Young people are prime targets**

  Scammers know you're online a lot, and they're getting smarter. They use fake giveaways, job offers, influencers, and even fake banking apps.

- **Cybercriminals don't need to break into your house**

  They just need you to trust the wrong message or app.

Co-funded by
the European Union

Why this matters

Your phone is now your wallet - you shop, send money, and manage your bank account from it.

But with great convenience comes serious risk. One wrong tap can open the door to scammers, and young people are being targeted more than ever before.

That’s why financial literacy is a must-have skill in today’s world.

- **One bad click = stolen money or identity**
- **Scammers now focus on young people — not just the elderly**
- **Your digital habits affect your financial safety**
- **Learning the basics = protecting your future**

Being smart with your money starts with knowing how to spot risks and avoid costly mistakes.
Don’t wait until it’s too late!

Co-funded by
the European Union

FinaLY

What you'll learn today

- ✅ How to spot safe websites and payment methods
- ✅ How to create strong passwords
- ✅ How to recognize online scams
- ✅ How to use Revolut, PayPal & finance apps wisely
- ✅ How to protect your personal data online

Co-funded by
the European Union

What are safe online practices?

Staying safe online isn’t just about avoiding viruses - it’s about protecting your **money, identity, and future**.

Here are some essential habits every young person should follow:

- **Shop only from secure, trusted websites**
  Look for “https://” and avoid sketchy deals that seem too good to be true.
- **Keep your financial info private**
  Never share your card details, PINs, or passwords - even with friends.
- **Reduce the risk of fraud or theft**
  Use strong passwords, enable two-factor authentication, and avoid public Wi-Fi for money-related actions.
- **Double-check before tapping “Pay,” and always review your bank statements for suspicious activity.**

Co-funded by the European Union

How to spot secure websites

Before you enter any personal or payment info online, make sure the website is safe.

Here’s how to tell:

- **Look for “https://” in the URL**
  The “s” stands for secure - never trust sites without it.
- **Check for a padlock icon in the address bar**
  This means the site has an SSL certificate and encrypts your data.
- **Stick to well-known and trusted websites**
  If you’ve never heard of it and it looks sketchy, trust your gut - don’t risk it.
- **Watch out for strange pop-ups, typos, or bad design**
  These can be red flags that the site isn’t legit.

✅ https://www.trusted-shop.com
❌ http://www.trust3d-sh0p-deals.example

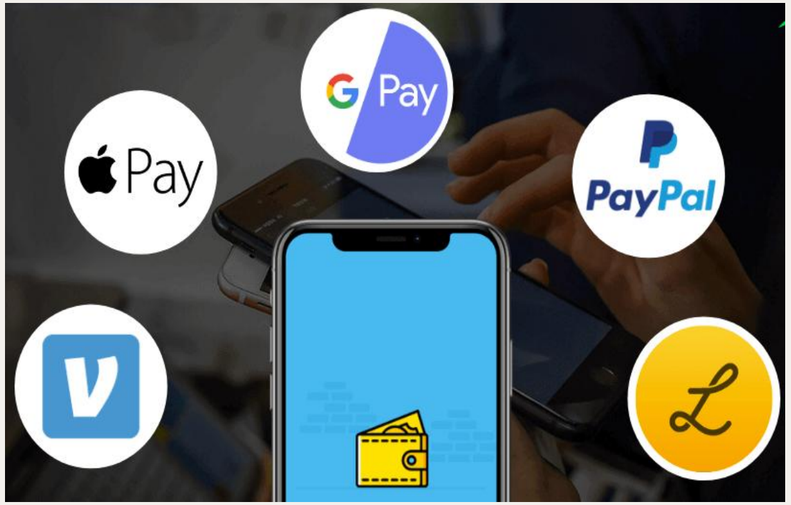
Co-funded by the European Union

Safe payment gateways

Not all payment methods are equally safe. Choosing the right one can protect both your money and your personal information.

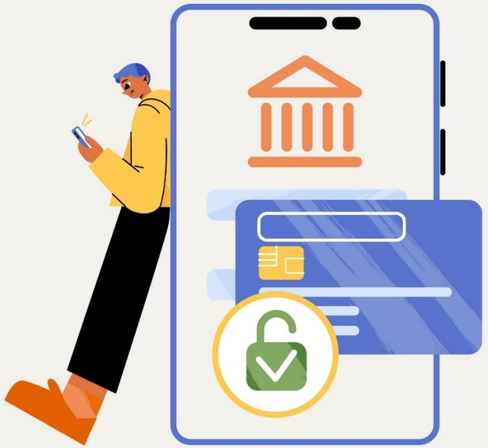
Here’s what to keep in mind:

- **Use secure, trusted payment methods**
  Stick to platforms like PayPal, credit/debit cards, Apple Pay, or Google Pay - they offer built-in security and buyer protection.
- **Confirm payments directly on the official platform**
  Always complete transactions within the website or app.
  Never through outside links or pop-ups.
- **Avoid payments by email, text, or phone**
  If someone asks you to send money this way, it’s a major red flag - it’s often untraceable and unsafe.
- **Keep digital receipts and track transactions**
  Screenshots or confirmation emails can help if there’s ever a dispute.



Co-funded by
the European Union

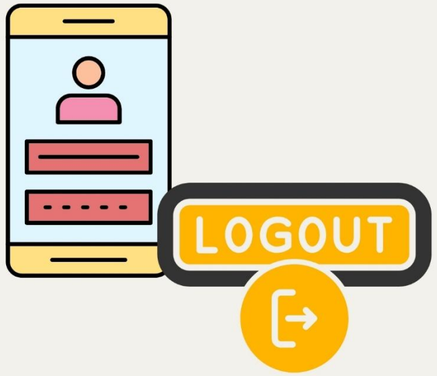
Tips to stay safe online



1. Keep your **antivirus software up to date**: It helps block malware, phishing attempts, and suspicious downloads.

2. Password safety: Use **strong, unique passwords** for every account, avoid reusing them, and update them regularly.

3. Monitor your bank account for **unusual activity**: Check your statements often and report anything that looks off immediately.



4. Enable **two-factor authentication** (2FA): An extra layer of protection for your email, social media, and banking apps such as:
   - Face ID / Fingerprint (biometrics)
   - One-time codes sent by SMS or email
   - Authenticator apps (e.g., Google Authenticator, Microsoft Authenticator, Authy)
   - Security keys (like YubiKey or Titan Key)

5. **Log out** when using shared or public devices: Don’t let others access your accounts by accident.

What is password hygiene?

Password hygiene means using smart habits to keep your accounts safe.
It’s your first line of defense against online threats.

Best Practices for strong and secure passwords:

- **Make it long and complex:** Use at least 12 characters including uppercase and lowercase letters, numbers, and symbols (e.g., *M!cr0S@fe2025!*)
- **Never reuse passwords:** One hack = access to everything if you’re using the same password across sites.
- **Avoid easy-to-guess info:** Skip names, birthdays, pet names, or anything someone could find on your social media.
- **Enable Two-Factor Authentication (2FA):** Add an extra layer of security by requiring a second step (like a code from your phone or an authenticator app) in addition to your password.
- **Keep recovery options updated:** Ensure your backup email & phone number are current.
- **Use a trusted password manager:** Stores all passwords securely and encrypts them.
- **Avoid plain text storage:** Don’t keep passwords in notes apps, emails, or sticky notes.

Co-funded by
the European Union

Tips for strong passwords you can remember

1. Replace letters with numbers or symbols
Take a word or phrase you can easily remember and replace some letters with similar-looking numbers or symbols.
For example:
Word: "sunflower"
Password: sun310w3r

2. Combine unrelated words
Pick 3-4 random words and combine them. The more unusual the combination, the better.
For example:
Words: book, cheese, tree
Password: BookCheeseTree

3. Use a memorable date with a phrase
Combine a significant date with a phrase related to that date.
For example:
Event: Wedding anniversary on June 15, 1980
Password: WeddingDay15061980
Note: Avoid using just a memorable date and avoid the sort of information someone might be able to get from somewhere like Facebook, such as your birthday.

4. Use the Name-Date-Place method
Combine the name of someone important to you, a significant date, and a meaningful place.
For example:
Name: Mary
Date: Born in 1950
Place: (had our honeymoon in) Cambridge
Password: Mary1950Cambridge

Source: AbilityNet. (2025, February). *Tips for creating strong passwords you can remember*. AbilityNet. https://abilitynet.org.uk/factsheets/tips-creating-strong-passwords-you-can-remember

Co-funded by the European Union

Password Strength Chart

SANDSTORM IT power on

This is based on the average brute forcing (botnet) power in 2019.

123456 Top 10,000 password	**0.20 milliseconds**	**Unsafe**
qwerty123456 Longer "common" password	**13 hours**	**Unsafe**
ITFunSom3times Longer password with numbers	**48 thousand years**	**Risky**
ITifun0m3times! Longer password with numbers and special characters	**13 trillion years**	**Good**
imusingalongpasswordtoday Even Longer password	**913 trillion years**	**Better**
imu$inga1ongpa$$word+oday! Even Longer password with numbers and special characters	**2 octillion years**	**Best**

Please Note: These passwords are for demonstration purposes ONLY and are not to be used.

What are scams and fraud?

Scammers are everywhere online - and their goal is simple: trick you into giving up your money or personal info.

- **Phishers and fraudsters target your trust**
  They pretend to be banks, delivery services, or even friends to get your data.

- **They use fake emails, messages, or links**
  These may lead you to look-alike websites or ask you to “verify” your info.

- **They often promise things that seem too good to be true**
  Like free iPhones, gift cards, or easy money - it’s almost always a trap.

- **If something feels off - pause and double-check**
  Better safe than sorry when it comes to your online safety.

Co-funded by
the European Union

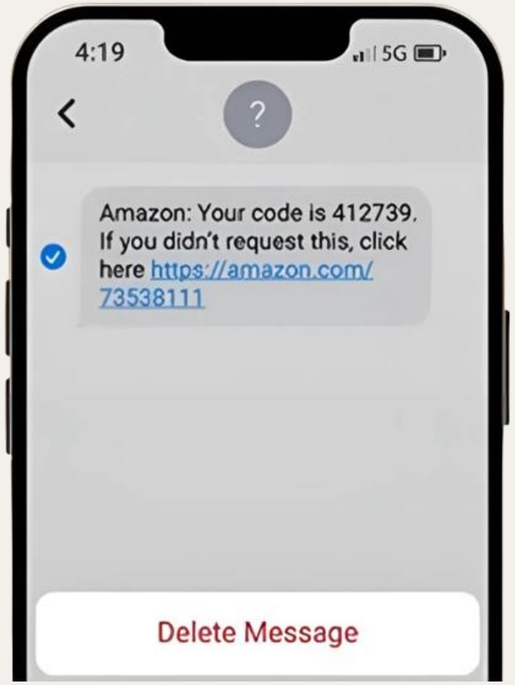
How to spot phishers

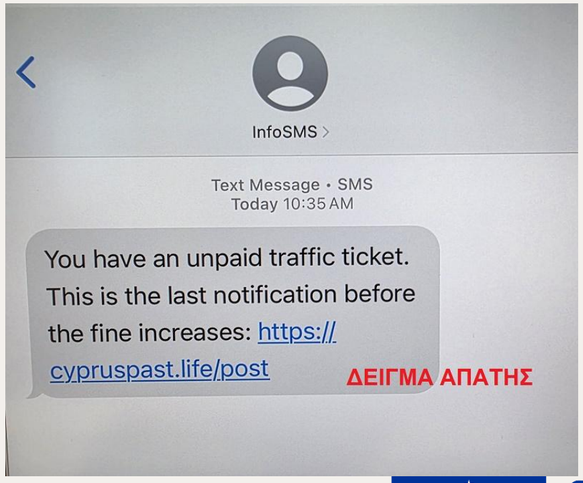
Check the sender’s email address
Is it misspelled, unfamiliar, or slightly off? That’s a red flag.
(e.g., support@paypall.com)

Look out for urgent messages or threats
"Your account will be closed!" or "Act now!" - pressure tactics are classic scam moves.

Be careful with suspicious links or attachments
Hover over links before clicking - if it looks weird, don’t open it.

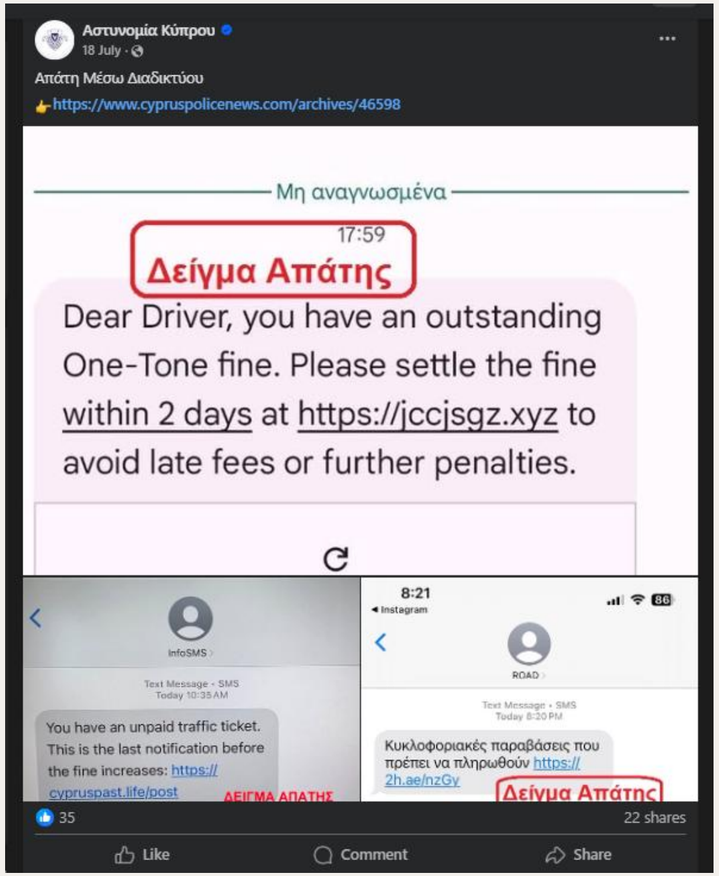
Think before sharing personal or financial info
No legit company will ask for your passwords or credit card info via email or text.





Co-funded by the European Union

Cyprus Police News

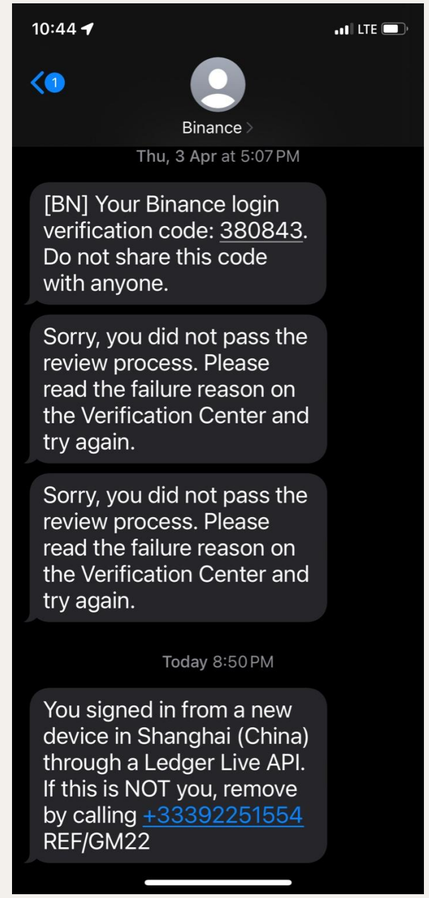


Co-funded by the European Union

How to spot phishers

The last message in the screenshot is **a scam**.

- **Urgency and Fear Tactics**: It claims a login from a suspicious location (Shanghai, China), which is a common scare tactic to prompt quick action.
- **Suspicious Phone Number**: It asks you to call a non-Binance number (+33392251554). Legitimate companies like Binance do **not** ask users to call random international numbers for account security.
- **Unusual Reference Code**: The use of a "REF/GM22" code adds to the fake urgency and legitimacy. This kind of phrasing is typical in phishing messages.
- **Inconsistency in Message Style**: The legitimate Binance messages above it are clear, concise, and don't ask you to take actions like calling a number.



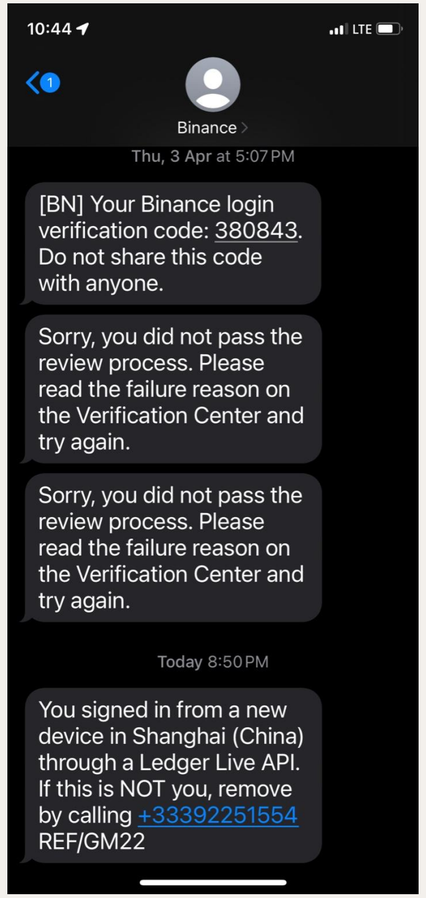
What to do:

- **Do not call the number.**
- **Do not click any links** if the message had any.
- **Report the message to Binance Support** immediately via their official website.
- Consider enabling **2FA (Two-Factor Authentication)** and changing your Binance password just in case.

Co-funded by the European Union

How to spot phishers

Scammers can **spoof sender IDs**, meaning they can make a fake message **appear under the same thread** as legitimate messages (like those from Binance).



How They Do It:

- **Sender Spoofing**: The scammer uses software to send an SMS that appears to come from “Binance.” SMS systems aren't always secure against this kind of trick.
- **Automatic Threading**: Your phone groups messages by sender name/ID. So if the spoofed name matches “Binance,” your phone threads it with legitimate messages, even if it didn’t actually come from Binance.

Why It’s Dangerous:

- It looks more trustworthy because it appears in the same conversation.
- People assume it must be real because it’s grouped with past legitimate alerts.

What to Do:

- Always check **official channels** (Binance app, website, or verified support email) rather than trusting SMS content.
- Never call or click anything in a message unless you’re absolutely sure it came from a legitimate source.

Co-funded by the European Union

Staying safe online

- ✅ Always **think before you click**
- ✅ Keep your **devices and antivirus updated**
- ✅ Report suspicious messages or emails
- ✅ When in doubt - **ask for help** (parents, bank, or authorities)

Co-funded by the European Union

Digital Wallets

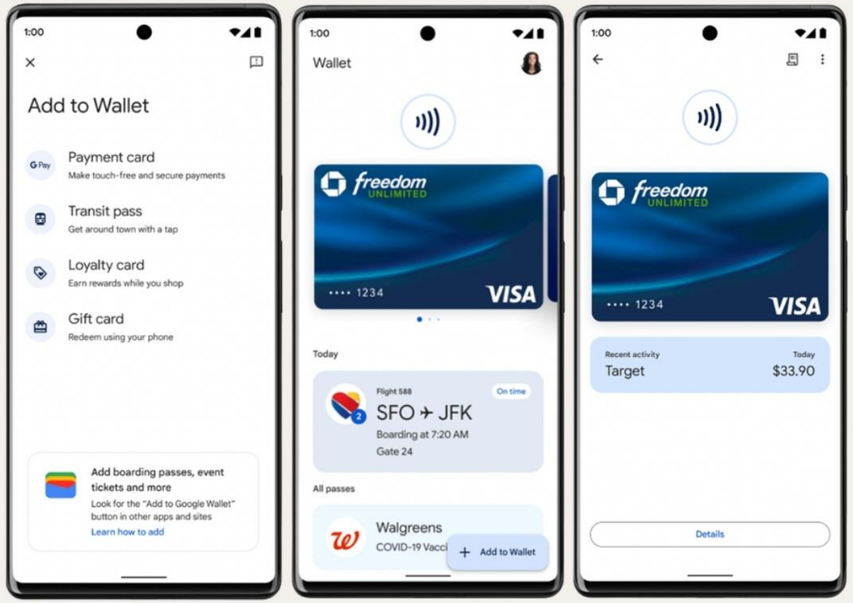


Image: Google
YouTube: Phone, keys... Google Wallet | Google
https://www.youtube.com/watch?v=3eKF_kEjy-I

➢ What Is a Digital Wallet?

A digital or electronic wallet is an **app or software** that securely stores your payment information, such as credit, debit, or gift cards and sometimes even other items like loyalty cards, tickets, ID, and cryptocurrencies.

➢ How It Works

- Once you add your card, transactions use **tokenization**, which replaces your real card details with a unique token. This keeps your data safe, even if a store is hacked.
- Payments are confirmed using secure **authentication methods** like Face ID, Touch ID, or a PIN.

➢ Everyday Examples

- **Apple Wallet / Apple Pay** – Store and use cards, IDs, and passes seamlessly and securely.
- **Google Wallet / Google Pay, PayPal, Revolut** – Popular digital wallets offering contactless payments, transfers, and money management.

Benefits of Using Them

- **Super fast & convenient**
  Pay instantly without carrying cash or cards.
- **Track your spending in real-time**
  See exactly where your money goes - right from your phone.
- **Get instant payment notifications**
  Can confirm that your payment has gone through and how much you were charged
- **Perfect for online shopping & travel**
  Shop worldwide safely and pay in multiple currencies.
- **Easy to split bills with friends**
  No more awkward IOUs - share expenses instantly.

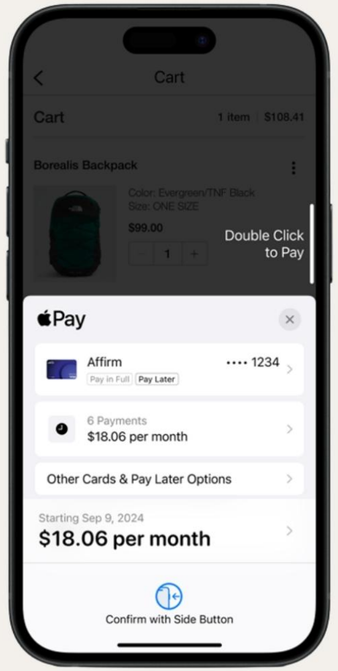


Image: www.apple.com/apple-pay/

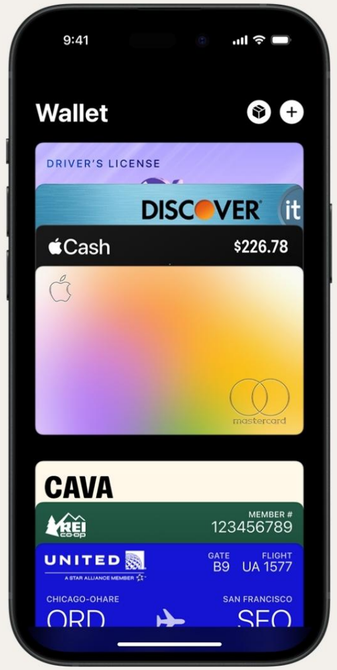


Image: www.apple.com/wallet/

Image: www.revolut.com/apple-and-google-pay/

How to Use Them Safely

- Use strong device security. Lock with Face ID, fingerprint or PIN
- Turn on notifications for every transaction
- Use two-factor authentication (2FA) and strong passwords
- Download only official apps – From Google Play or App Store
- Avoid public Wi-fi for payments – Use mobile data or a secure transaction

Co-funded by
the European Union

Smart Money Habits

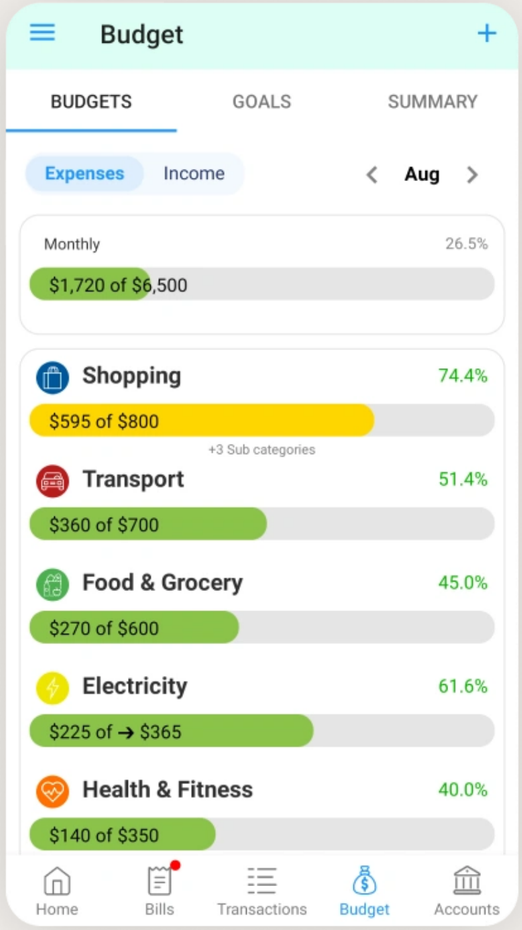


Image: www.timelybills.app/budgeting-app

Co-funded by the European Union

What is data privacy?

Data privacy means knowing how your personal and financial information is used, stored, and shared - and taking steps to protect it.

Your personal and financial info = sensitive
Details like your name, location, bank info, and spending habits must be kept secure.

Apps and banks collect data to provide services
They track your activity to improve features - but you have a right to control what they access.

Know what you're sharing - and with whom
Always check privacy settings, terms of use, and permissions before using an app or service.

Co-funded by
the European Union

What info should you protect?

- Full name & address
- Bank card or account details
- ID numbers (passport, national ID)
- Login info (emails, passwords)
- Spending habits & transaction history

How to stay in control

You can’t stop all data collection - but you *can* decide who gets what.

How to stay in charge of your digital footprint:

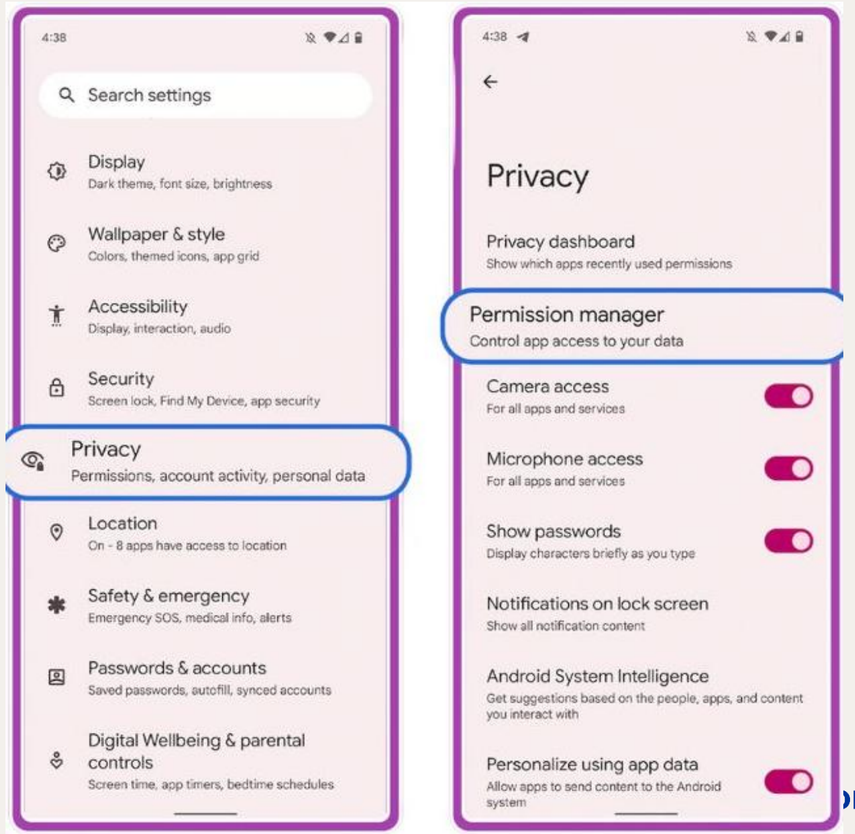
- **Only share info on secure, trusted platforms**
  If it looks shady, it probably is - don’t risk it

- **Check privacy settings in every app**
  Limit what apps can access (like contacts, photos, or your camera)

- **Read what you’re agreeing to**
  Terms, conditions, and permissions matter

- **Turn off location access when not needed**
  Your phone doesn’t need to track you 24/7

- **Be mindful of what you post online**



How platforms should protect you

It’s not just up to you - platforms also have a responsibility to keep your data safe.
Responsible platforms should always provide the following protections:

Use encryption to protect your data
Your info should be locked down so no one can access it without permission.

Let you update or delete your personal data
You should have control over what stays and what goes.

Be transparent about how your data is used
No hidden tracking - you deserve to know exactly what’s being collected and why.

Provide privacy policies in simple language
No legal jargon - just clear, easy-to-understand explanations of your rights.

Co-funded by the European Union

What are financial regulations?

They protect consumers:
Regulations help prevent scams, fraud, and unfair practices

Ensure banks & financial apps are safe and fair:
They must follow strict standards when handling your money

Enforced by financial authorities:
Organizations like **Central Banks or Financial Regulators** monitor how money systems operate

Co-funded by the European Union

How they protect you

- ✅ Stop scams and illegal activity
- ✅ Make companies follow privacy & security laws
- ✅ Ensure your money is handled responsibly
- ✅ Offer support when companies break the rules

Co-funded by
the European Union

What are safety nets?

A **safety net** is protection that helps you when unexpected problems happen.

Types of Financial Safety Nets

1. **Emergency Savings:** Money set aside for sudden expenses (e.g., medical bills, car repairs).
2. **Insurance:** Health, car, or home insurance protects you from large unexpected costs.
3. **Government Programs:** Benefits like unemployment aid or pensions support people in hard times.
4. **Support Systems:** Family, community, or social groups that provide help when needed.

Why Safety Nets Matter

- Reduce stress and financial risk.
- Help you recover faster from setbacks.
- Give peace of mind and stability.

Co-funded by
the European Union

Know the limits

Financial regulations help - but they don’t cover everything
It’s important to stay aware of what *isn’t* protected!

Not every app or platform is regulated
Some tools may look legit but operate outside the rules

Crypto & foreign websites may lack protection
If something goes wrong, it’s harder to get your money back

You still need to stay alert and informed
Read reviews, do your research and know the risks

Smart + Safe = Your best protection
The more you know, the better you can protect your finances.

Co-funded by
the European Union

WRAPPING UP

FinaLY

Co-funded by
the European Union

Training Seminars

All participants are entitled to register for FREE training:

Participation:

- Physical (Cyprus and Ireland)
- Online

Sessions:

- 4 online webinars
- Physical Hands-on workshops
- Discussions
- Certification of participation

* Each participant should complete a feedback form at the end of each bootcamp

Co-funded by
the European Union

Feedback and courses

We would be grateful for your feedback, in order for us to improve future training sessions

SCAN HERE

The class365 platform contains all educational material in Greek and English, including recordings, resources and tools

www.class365.eu www.learn.finalyproject.eu

SCAN HERE

Co-funded by the European Union

For more information:

www.finalyproject.eu/
www.facebook.com/finalyproject
www.instagram.com/finalyproject/
www.tiktok.com/@finalyproject?lang=en

ecect.projects@gmail.com
+ 357 96520112 (Cyprus)

Co-funded by
the European Union