Rialtas na hÉireann
Government of Ireland

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

How to keep your online accounts secure

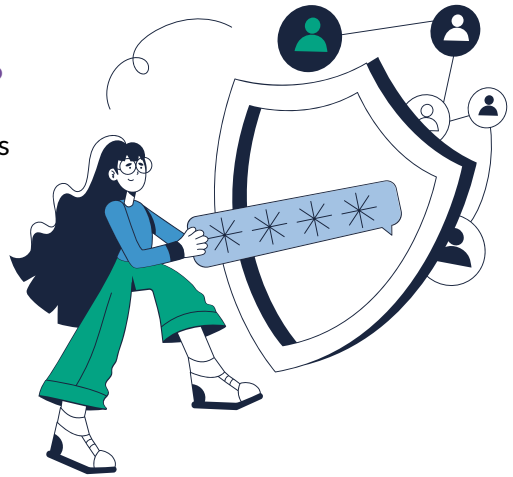
Advice from the National Cyber Security Centre

This is an important booklet that will help you keep your online accounts safe. We use some specialist words you need to know when using online accounts or smartphone apps. We explain these words in the handy glossary on pages 9 to 11.

ncsc.gov.ie

Plain English
Approved by NALA

Why should I keep my online accounts secure?



You should keep your online accounts secure so you can protect private information, like your:

- personal details
- bank account
- social media
- purchase history.

When you follow the advice in this booklet, you can:

- protect and secure your online accounts
- reduce the risk of being hacked.

How can I make my online accounts secure?

You can make your online accounts and smartphone apps more secure by using a strong password or passphrase. A password or passphrase should be a secret that only you know.

They are like locks you put on valuable things. You will want to use the strongest lock possible to keep valuables safe.

Are passwords and passphrases the same?

Yes, but a passphrase is an easier way to remember a strong password.

A strong password has at least 12 characters - 14 or more is better.

By characters, we mean it **should** contain a mix of:

- numbers
- letters in CAPITALS and lowercase
- special characters like !,£,%,*

For a password, **never** use:

- real words or words in a dictionary – it's best to invent them!
- names, birthdays, or addresses
- the same username and password for more than one account
- patterns like 12345678 or Ireland123

Try to make the password difficult for a hacker to guess.

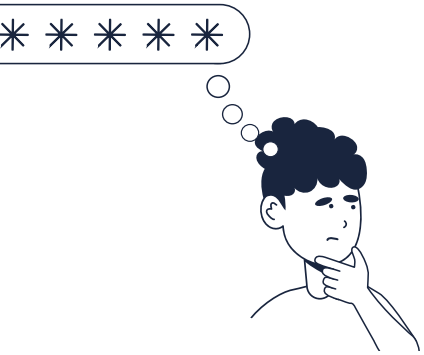
A strong passphrase contains at least 3 words – 4 or more is better.

The words you choose should be random, **but** pick words that will be easy for you to remember and hard for others to guess. For example, don't pick 'matchesgolftennis' if these are your hobbies. These might be too easy to guess.

A passphrase should also have a mix of characters.

A long passphrase can be easier to remember than a password.

`loNg*passworDs*ruL3!`



Never share your password or passphrase

Your password or passphrase is a secret that only you should know.

Remember, a real customer service or helpdesk staff member will never ask you for your password, passphrase or PIN.

Only a scammer will ask for your password, passphrase or PIN.

Avoid using the same password or passphrase

You need to use different passwords and passphrases for each of your important online accounts and apps. This will stop a hacker from getting into your other important accounts if they find out one of your passwords or passphrases.

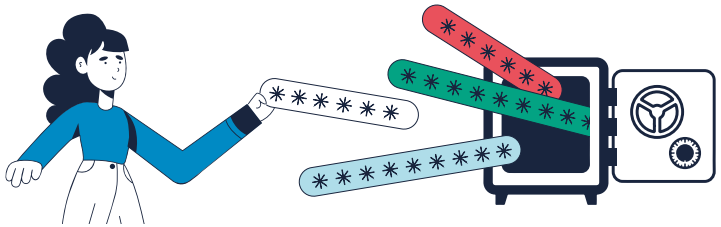
Some new approaches to account security

What is a password manager?

This is a software program that allows you to create strong passwords for all your important accounts and store them in one place online. It is like an online safe.

Many password managers work with internet browsers and smartphone apps. They allow your device to automatically fill in the username and strong password.

If you decide to use one, you will only need to remember one strong password to access the password manager. It is essential to have **2FA** or **MFA** switched on for your password manager. We explain these on the next page and in the glossary on page 10.



What are 2FA and MFA?

Two-factor authentication (2FA) or multi-factor authentication (MFA) are ways to make your online accounts much safer.

Think of it as having two locks on your door instead of one.

We recommend you use 2FA or MFA for important accounts and services.

After entering the password for your account, you will also need to enter a code sent to your phone, app or email.

Never share this code with anyone.

Services that use 2FA or MFA

Many services like MyGov.ie, online banking and social media automatically offer 2FA or MFA.

What is a passkey?

Passkeys are beginning to replace passwords.

A passkey allows you to securely login to online accounts or smartphone apps without having to enter a username or password. Passkeys use your fingerprint or face ID on your smartphone to unlock the account or app you are logging into.

When you are creating new accounts, many will suggest using Passkeys or 2FA or MFA. You should use them.

What about your existing online accounts?

To check or use passkeys, or 2FA or MFA, you will usually find these in the settings or in the security section of the online account or app.

Final top tips

1. The longer your password or passphrase, the stronger it is:
   - use a minimum of 12 characters, but 14 or more is better
   - use a mix of characters.
2. A password or passphrase should be a secret that only you know – never give it away.
3. Use different passwords or passphrases for each of your important accounts.
4. Use 2FA or MFA to secure your accounts, when it is available.
5. Never give your 2FA or MFA code to anyone.

Words and names you need to know when using online accounts or smartphone apps

Words and names	What it means
Application or app	Apps are software programs designed to do a specific job. They allow you to carry out specific tasks on a mobile or desktop device.
Authentication	This is a process that confirms the identity of a user or what they are doing.
Authenticator app	An Authenticator app is an app that you install on your phone. It creates temporary codes that you use as an extra layer of security when logging into websites or apps. See MFA or 2FA.
Lowercase and uppercase letters	In English, lowercase letters are like this: a, b, c, d, and so on. Uppercase (sometimes called capital letters) letters are: A, B, C, D, and so on.
Face ID	This is a way of identifying or confirming a person's identity using their face.
Fingerprint	These are unique patterns that appear on the pads of the fingers and thumbs. Computers and mobile devices can use them to identify people.
Hacked	Your account is hacked when a person or system has access to your data or account without your permission.
Internet browser	An internet browser is a software program that lets people access web pages on the World Wide Web.

MFA (Multi-factor authentication) or 2FA (Two-factor authentication)	MFA or 2FA uses your username and password and other pieces of information like a: • PIN (see below) • fingerprint • one-time password (OTP) from an authenticator app. It will then give you access to online accounts.
NCSC	The National Cyber Security Centre.
OTP (One-time password)	An OTP authenticates you for a single login with a password or code that you cannot reuse.
Numbers	These are the digits on your keyboard or phone: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.
Online account	This is an online service that you access on the internet.
PIN (Personal identification number)	A PIN is a number code you use to confirm your identity when: • logging in to online accounts • making ATM withdrawals • making credit-card payments.
Passkeys	Passkeys are replacing passwords and passphrases. They are a new way of allowing you to log into your accounts by using the Face ID or Fingerprint features on your phone to approve the login.

Passphrase	A passphrase is a password that is made of random words, which is easier to remember than a password.
Password	This is a secret word or phrase that you use to allow access to a computer system or service.
Password manager	This is a software program that allows you to create and store strong passwords for different online services.
Scammer	A scammer is someone who makes money using illegal methods. They do this by tricking people into sharing their usernames and passwords. They then use these to access your online accounts.
Online security	This is what you do to stay safe when online.
Smartphone app	This is a software program used on smartphones.
SMS (Short message service)	This is a text message received by phone.
Special characters	These are keyboard keys that are not letters or numbers. They are symbols like: !,£,%,*
Two-factor authentication (2FA)	This means using your username and password and one other piece of information like a PIN, fingerprint or code from an authenticator app. This then gives you access to your account.

Where can I find out more?

Visit the National Cyber Security Centre website for up-to-date information and to find other resources that will help you to keep your online accounts secure.

ncsc.gov.ie

Rialtas na hÉireann
Government of Ireland

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre