

# Safety first



## How can I be safe online?

The internet is a great place. You can meet new people, contact people you already know, learn an incredible amount of stuff and have a great time. But you must **always be careful**, because there are large and small risks lurking around. BOO!

# The risks to your computer

Just like you have to be careful when you're walking around, you must also **keep an eye on things when you're online**. Because when malware like a Trojan horse gallops into your computer, programmes and people with bad intentions can look inside and abuse your data.

## How does that work?

- Through ordinary websites that are '**contaminated**'
- Through software that is **not up to date**
- Via '**v**' **attachments** in your e-mail
- Through social media accounts that are **poorly protected**
- Because you **don't use an antivirus programme** and/or firewall

But the latter can be fixed in no time.

Did you know Windows automatically comes with the programmes **Windows Defender** and **Windows Firewall**?

### Danger zone!

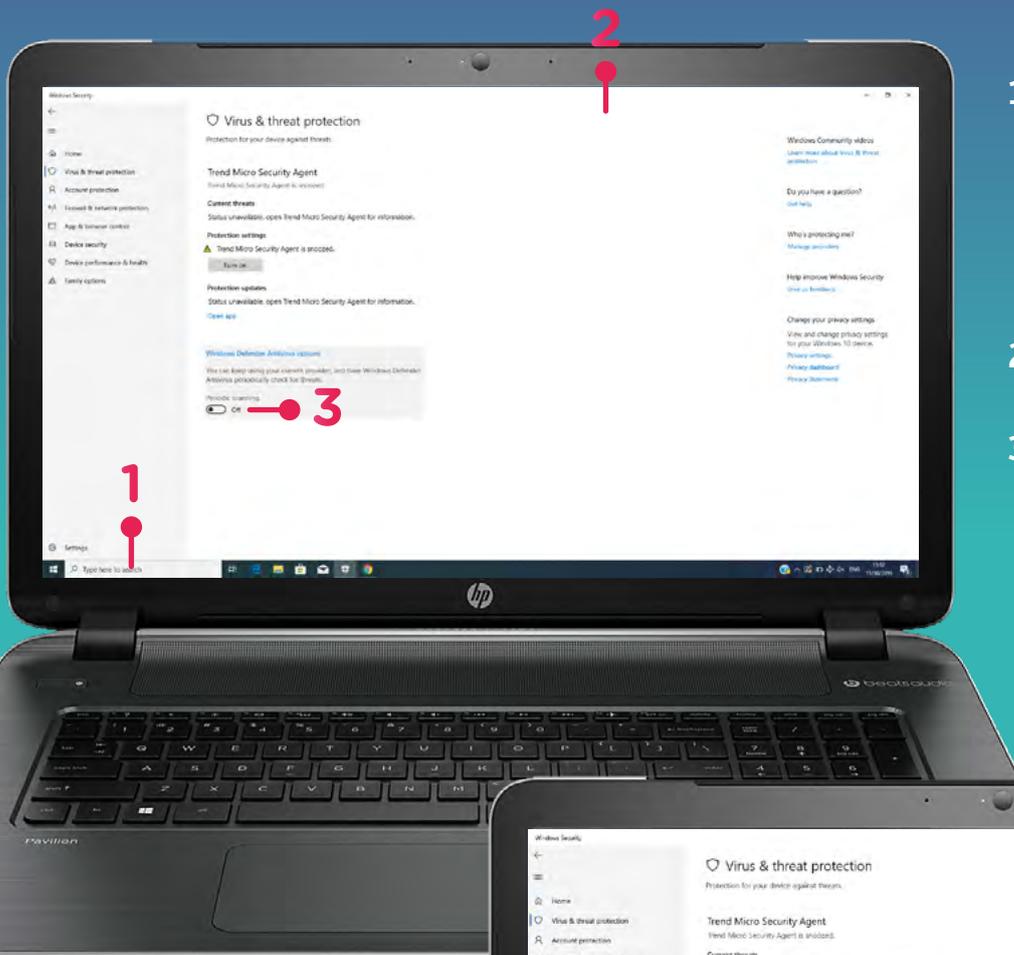
Malware is the collective name of all kinds of malicious software. It can seriously mess up your computer and even collect sensitive information. Your passwords, for example! Creepy stuff. 🧛

An example of this is a 'Trojan Horse', which looks like something very reliable, something you think you know. But as soon as you let the horse in, it kicks and stomps around. And does a lot of damage in your computer booth.

**Forewarned is forearmed!**



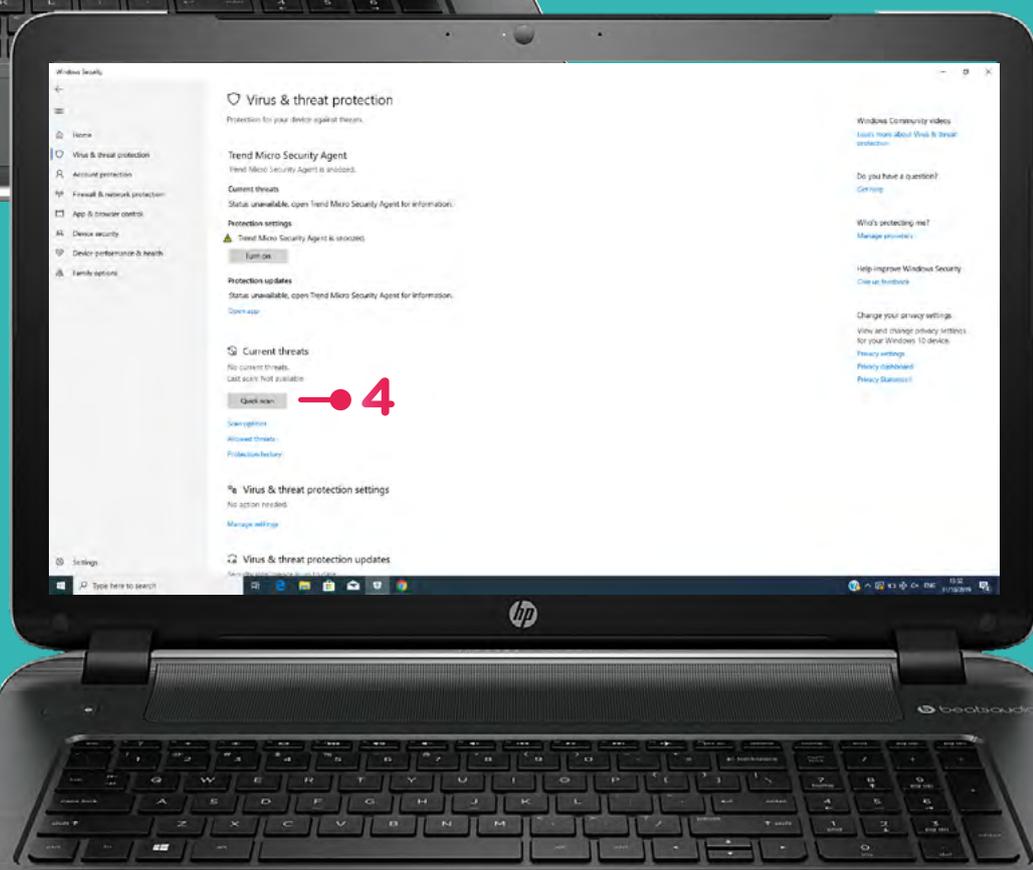
# How does Windows Defender work?



- 1 Type 'Windows Defender' in the search field in the left corner of your desktop and press Enter (if you work with Windows, obv).
- 2 Here's what Windows Defender looks like.
- 3 If it says 'disabled', click 'Settings' in the upper right-hand corner and tick 'Activate protection in real time (recommended)'. Now click 'Save Changes'.

- 4 Then go back to the first tab 'Homepage' and click 'Analyse now'. Now, the programme tracks infected files and you can delete them.

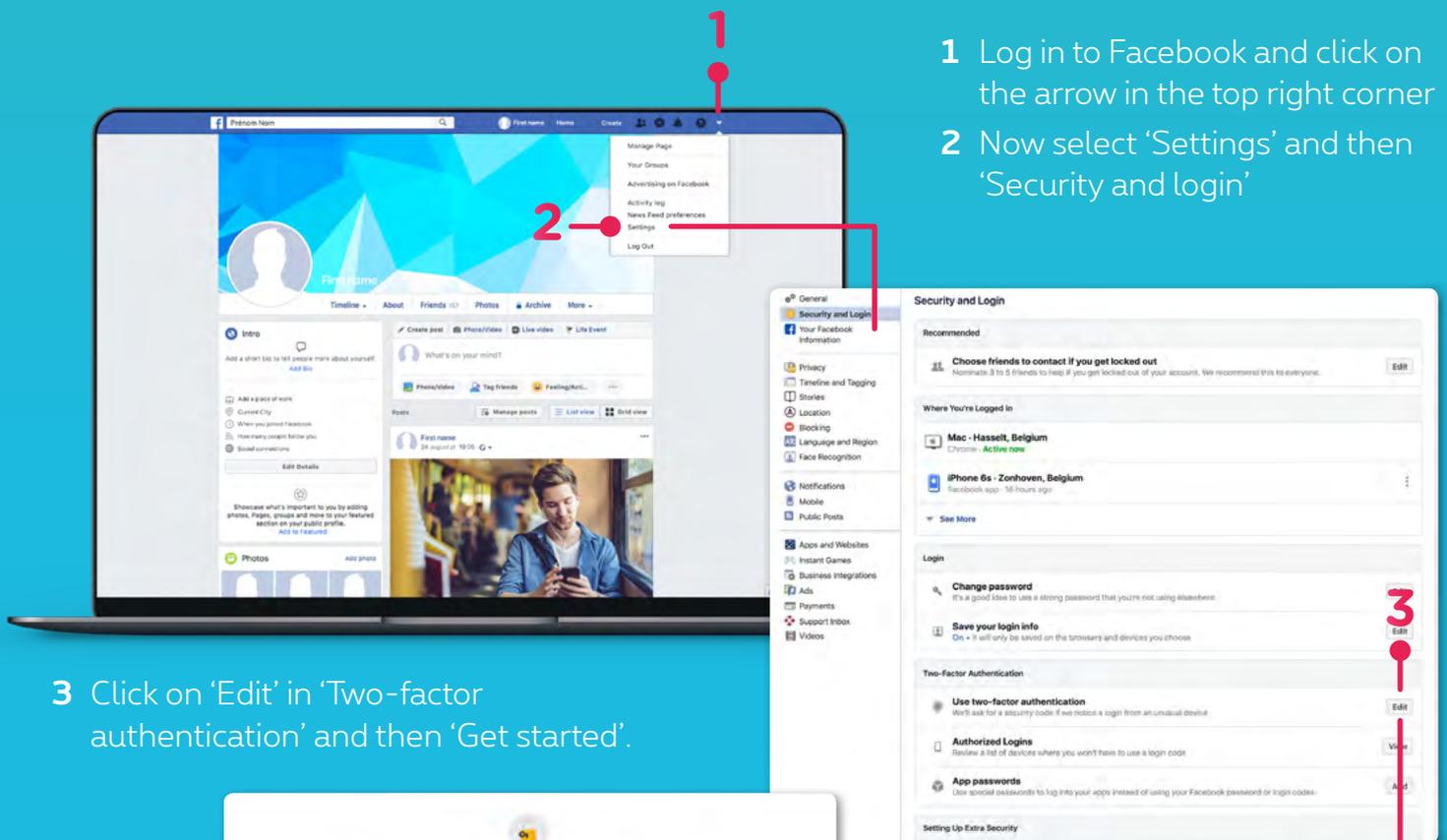
Phew, you saved your computer again! What a **digi-hero!** 🤖



# Safe on social media

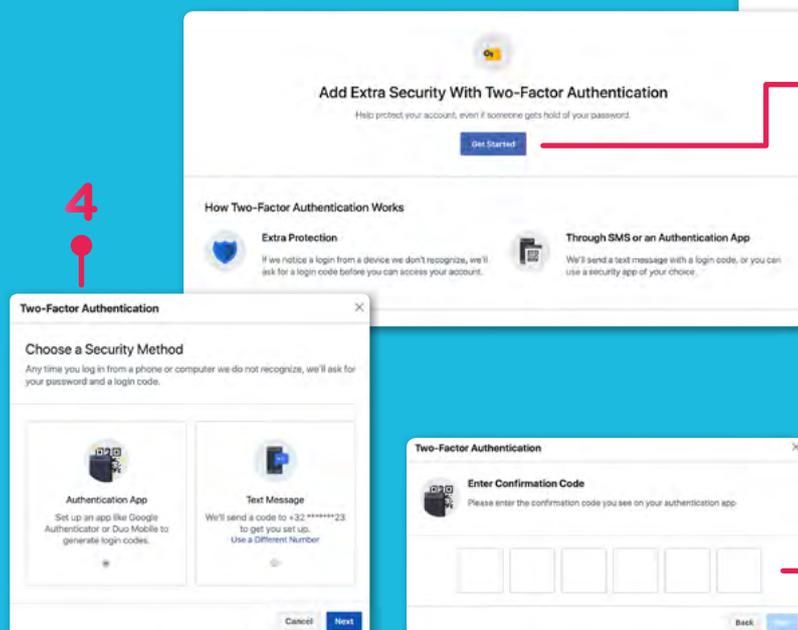
To keep people with bad intentions away from your social media, different platforms give you the option of **'Two-Factor Authentication'**. That's a difficult word but it's easy-peasy to configure. Let's check Facebook to explain how it works.

- 1 Log in to Facebook and click on the arrow in the top right corner
- 2 Now select 'Settings' and then 'Security and login'



- 3 Click on 'Edit' in 'Two-factor authentication' and then 'Get started'.

- 4 Check 'Text message' to receive the security code on your mobile and click 'Next'.
- 5 Now you get a code on the phone number you entered. Enter it. Click 'Next'. The two-factor authentication is up & running! Each time you log in from an unknown smartphone or computer, you'll get a code.  
**Extra safe!**



# Pass ... word!

A vital element  
of your online security  
is your **password**.

So, don't choose a password anyone  
else can easily guess, such as:

- Your own name (duh!) or your pet's (sorry, Cornelia the corgi!)
- Your date of birth or house number
- Logical rows such as 'abcdef' or '54321'.
- 'password'

**Important:** never keep a note with  
your password in a visible place! Just  
learn it by heart.



## Your password is top secret!

Never give your password to anyone else. **Never! Never ever! Never ever ever!** Not even to your BFF or BAE. You may be very close but your password is your very own top secret. You wouldn't share your toothbrush either, now would you?

## Strong, Stronger, Strongest

Sssht... don't tell anyone, but a strong password consists of at least 12 characters. It's best to make a good mix of upper and lower case letters, numbers and special characters. **MyDogB@rks20Times?** Easy to remember, hard to decipher!

## Safety tips for your computer

Here's a handy list:

- Never open an e-mail or an attachment that looks weird. Weird titles, no subject, unknown senders... Use your common sense!
- When you're on social, never click on a weird-looking link. Ask the sender if the link really comes from him!
- If a website asks you to enter personal data, always check there's an <https://> in the link at the top of your tab page. That means the site is well protected. And that your data is in safe hands.

# Would it? Could it?

So, how do you keep yourself safe on the internet? Of course, you know what's allowed and what isn't on the internet. But let's just say it one more time. You never know...

If you're not careful, you may come across people you'd rather not know. On the internet and in real life. It could be people who don't respect your boundaries, who are mean or even ask for money. Here's what you can do to deal with them.

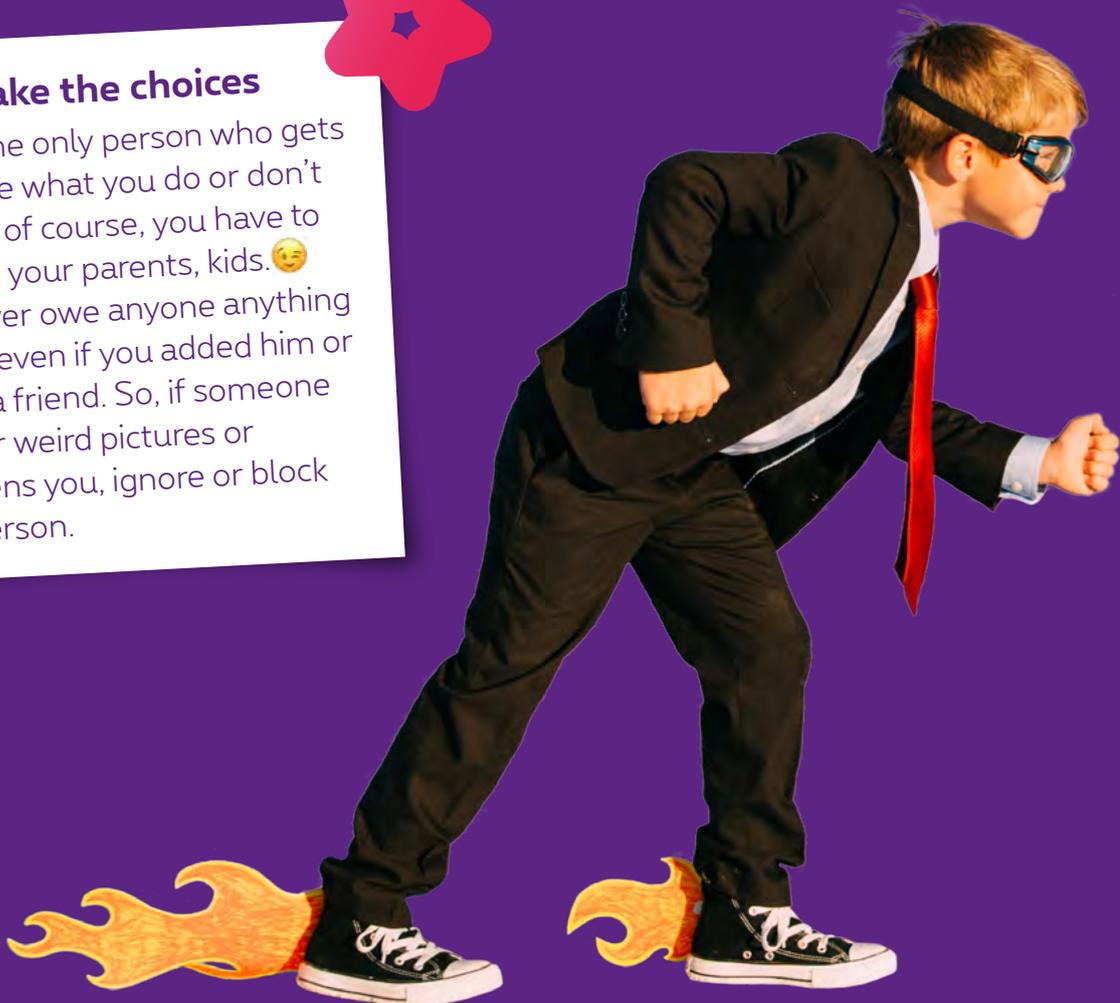
## On your marks, get set, go!

### You make the choices

You're the only person who gets to decide what you do or don't do. But, of course, you have to listen to your parents, kids. 😊 You never owe anyone anything online, even if you added him or her as a friend. So, if someone asks for weird pictures or threatens you, ignore or block that person.

### Sherlock!

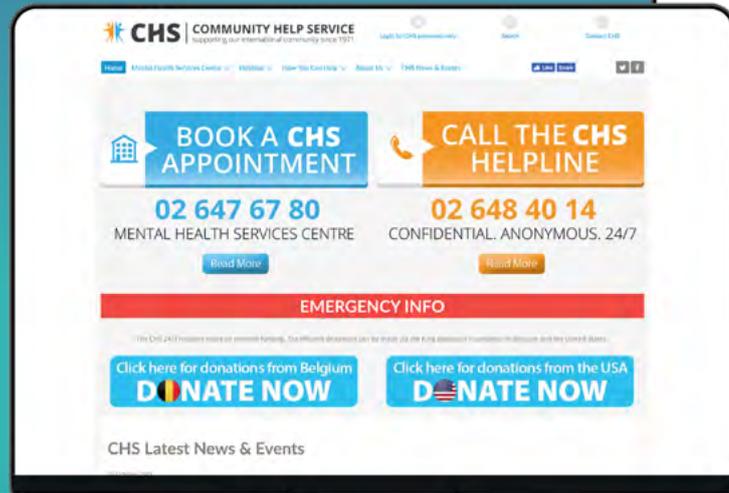
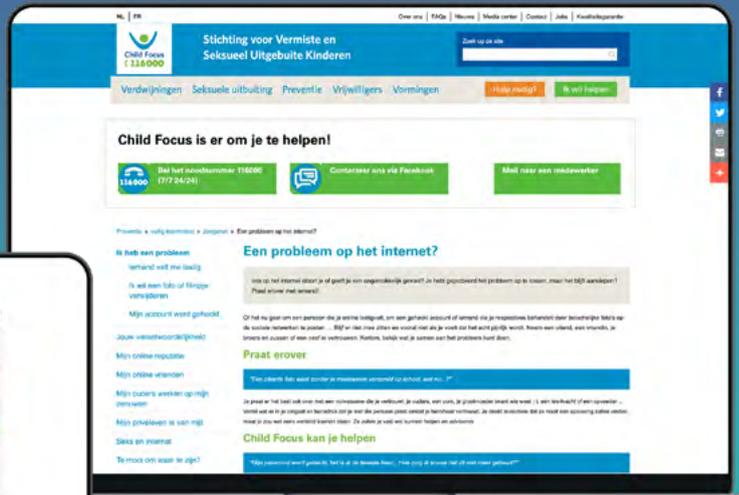
On the internet, there's a lot of information that is completely and utterly fake. #FakeNews. So use your common sense when you read something that sounds incredible. You can always double-check by asking your parents or by Googling it. Not sure how? Then go to **'Know-it-all'**! An e-mail can also have fake information. Ever got an e-mail saying some foreign prince wants to give you his fortune? Or that you won the lottery, without even playing? If it looks too good to be true, it usually is.



# Cyberbullying = no-go zone!

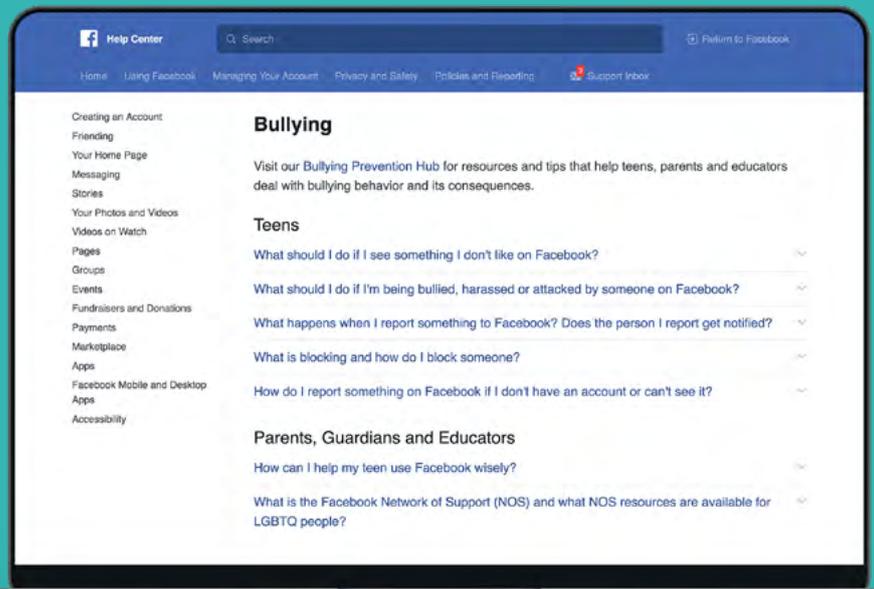
Is someone bullying or slandering you online? Then you can report that behaviour.

1 Talk to someone who listens to you and whom you can trust via the help line of **Child Focus**: via their website, by telephone at the toll-free number **116000**, by mail or on Facebook.



2 On the website **chsbelgium.org**, you can send an e-mail or chat with someone. You can also call them at the toll-free number **02 648 40 14**.

3 You can report it on the social media platform itself. On **Facebook**, for example, you can not only report bullying behaviour, you can even call on the help of a parent, friend or teacher.



## You're not alone.

Did you do something online that you're ashamed of or feel stupid about? Don't hesitate and talk about it with someone you trust 100%, so you can find a solution together. We all make mistakes, don't we?

# Can you diggit? Yes, you can!



proximus