Module 4:
Internet security & safety

Instruction kit for teachers

Short topic description

The Internet is a great tool for finding and sharing information, connecting with people and doing fun things. It's a world in which children are increasingly active today. They are very skilled in using it and don't always consider the risks to which they may be exposed.

In the module 'Internet security & safety' we highlight a number of Internet risks and how we can make children more resilient in case something goes wrong online.

Objectives

This module has the following objectives:

1. Understand the risks of viruses on computers, tablets & smartphones
2. Learn ways to secure computers and social media
3. Create awareness about assertive online behaviour
4. Provide means for reporting cyberbullying

ICT attainment levels

This module has the following ICT attainment levels:

- Pupils can use ICT in a safe, responsible and efficient way.
- Pupils can use ICT to communicate in a safe, responsible and efficient way.

In addition, attention is paid to the attainment levels for social skills.

- Pupils know how to be assertive with peers and adults by giving signals that are understandable and acceptable to others.

Module 4: **Internet security & safety**

Target group

- Primary education third grade
- Secondary education first grade

Tools

- Min. 5 computers / laptops with Windows 10 operating system
- Windows Defender Antivirus Software Package
- Internet access & web browser
- ‘Safety first’ diggit module

Duration

2 hours of lessons (2 x 50’)

Preparation

- Charge computers / laptops
- Prepare dummy information for creating a Facebook account
- Set up ‘Safety first’ diggit module on interactive board

Important terms and definitions

Below you will find an overview of a number of relevant terms and definitions regarding safe Internet use:

Worm

A worm is a computer program that multiplies. Copies of this worm are transmitted through the computer network without any user intervention. As a result, considerable damage is caused to all devices connected to that network.

The difference with a computer virus is that a worm spreads over the Internet, whereas a virus can't do this on its own. A computer virus needs a host, such as a file or e-mail, to spread (see also: Virus)

Firewall

A firewall is a security system used to protect your local computer network from unauthorized access.

Hacking

Hacking is breaking into someone else's or a company's computer(s) without permission by bypassing security. Hackers don't always intend to obtain information illegally; they usually want to show that the network is not sufficiently secure. Companies often employ ethical hackers to detect holes in the security of their computer networks. They want to contribute to the fight against cybercrime and are therefore the good guys of the Internet.

Internet troll

An Internet troll is someone who deliberately publishes messages anonymously on the Internet in order to sow discord. The messages can be about relatively innocent matters but can also take the form of provocative opinions.

Important terms and definitions

Below you will find an overview of a number of relevant terms and definitions regarding safe Internet use:

Malware

Generic name for **malicious and or harmful software**. The word is a contraction of 'malicious software'. Examples of malware are viruses, worms, Trojan horses and spyware.

Spyware

Spyware is the name for computer programs that collect information about a computer user and transmit it to someone else. The goal of spyware is usually to make money. The term comes from the word spy and the suffix ware, indicating that it is software.

Trojan horse

A computer program that looks deceptively real. Through a Trojan horse, viruses and worms are smuggled into the computer system, as well as invisible programs that collect confidential data on a computer and then send it to the sender of the Trojan horse who uses it for malicious purposes.

Virus

A virus is a computer program that can attach itself to a file on your computer. It enters undetected via a host, such as an infected file or e-mail. It is harmful because it takes up disk space and computer time on contaminated computers. In serious cases, a virus can also erase and disseminate sensitive information. In very serious cases, the user may even lose total control of the computer.

Interesting links

www.lokalepolitie.be/5412/vragen/criminaliteit-op-internet
www.veiligonline.be/
www.childfocus.be/nl/preventie/veilig-internetten/professionelen

Classroom script

Below, you will find an overview of the different steps in the lesson about safe Internet use:

5’ | **Part 1: Introduction**

15’ | **Part 2: Conversation starters**

15’ | **Part 3: Securing your computer**

45’ | **Part 4: Creating a strong password**

30’ | **Part 5: Being safe online**

Part 1: Introduction

1. Sketching the context: the Internet is a great tool, but there are also risks associated with it.
2. Explain the purpose of the lesson.

Part 2: Conversation starters

Pupils are often very active in the digital world so it's important for them to share their experiences. What do they do online? What do they find interesting? What goes right and what goes wrong sometimes? Getting the conversation started in class is one way of making pupils more digitally savvy. Below you will find a few questions that are meant as `conversation starters' for the topic 'Internet security & safety'.

- Imagine someone steals passwords from your Facebook and Instagram. What's the worst that could happen?
- A fake is someone pretending to be someone else. Someone who tries to get into your head and convince you to do weird stuff in front of the camera. So, how do you recognize a fake on, let's say, Facebook, Instagram or WhatsApp? What are your golden tips?
- Sometimes children break into each other's accounts and post a funny post on another person's Facebook page. They didn't mean to hurt anyone. But breaking into someone's account is a crime. What's the difference between a joke and criminal behavior on the Internet, in your view? When does it cross a boundary?

Part 3: Securing your computer

Short description

Computers connected to a network, no matter how small or big, are vulnerable to malware. Users should be aware that the way they handle their computers, files or e-mails can make a significant difference in the way they are exposed to these harmful influences.
In this part of the lesson we give you an insight into the risks of contamination of computers, tablets & smartphones.

Step-by-step

Contents per step	Methodology	Media
Assignment: Look up the definitions of the following words • Malware • Trojan horse • Hacking • Virus • Internet troll	Work in groups + classroom discussion	Google search

Contents per step	Methodology	Media
Explanation: There are several ways a computer gets infected: **1.** Through normal Internet sites that are themselves contaminated. **2.** Through software that is not up-to-date: make sure you update the software of your computer, tablet and/or smartphone as soon as you receive an update notification. **3.** Via infected attachments in an e-mail: **a.** you automatically receive them from friends or family, because their computers are also contaminated. **b.** you receive them from an – often unknown - sender with a clickable attachment **4.** Through social media accounts that are poorly protected. **5.** Because you don't use an antivirus program and/or firewall. **6.** Enter 'Windows Defender' in the search field of your computer window at the bottom left and press Enter. **7.** This is what Windows Defender looks like. **8.** If it says 'disabled', click 'Settings' in the upper right-hand corner and tick 'Activate protection in real time (recommended)'. Then click 'Save changes'. **9.** Next go back to the first tab, 'Homepage', and click 'Analyze now'. The program will track infected files and you can delete them. **10.** Your computer is now free of contamination.	Classroom teaching	Appendices 1 and 2

Contents per step	Methodology	Media
Task: Try this on the classroom computer now.	Work in small groups on the computer	
Question & answer: What can you do to better protect your computer? **Tips:** **1.** Never open an e-mail or an attachment that looks weird. For example: weird titles, no subject, unknown sender, errors in the text. Use your judgment and also check with an adult. **2.** Never click on a link that looks weird in an e-mail or social media post. Always ask the sender if it comes from him/her. **3.** If you're asked to enter personal data on a website, always check there's an https:// in the link at the top of your browser window. This way, you are sure the website is well protected and that your data is in safe hands.	Questions & answers + Closing with tips&tricks in classroom	

Part 4: Creating a strong password

Short description

A very important aspect of online security is choosing a strong password. This makes it harder for cybercriminals to break into your computer, tablet and/or smartphone. Some websites and apps go a little further, with 'two-step verification'.
In this part of the lesson, we'll teach you how to do that.

Step-by-step

Contents per step	Methodology	Media
Question: What is a WEAK password according to you? **Explanation:** A weak password is a password that someone can quickly guess **1.** Your own name **2.** The name of your pet **3.** Your date of birth **4.** Your street name and house number **5.** Logical patterns such as abcdefg or 12345678 Also: a written password is a weak password **1.** Tip number 1 : never write down your password on a note or post-it or in your calendar **2.** Tip number 2: never give your password to anyone else, even your best friend or girlfriend/boyfriend	Group discussion in class + overview with do's/ don'ts	Google search

Contents per step	Methodology	Media
Question: So, what is a STRONG password? **Explanation:** **1.** A strong password consists of at least 12 characters **2.** It consists of a combination of capital letters, small letters, numbers and special characters **3.** The combination is original: MydogB@rks20Times! **4.** It's in your head **5.** You have different passwords, because if something goes wrong with one of them, it cannot be used to penetrate all your social media, e-mail accounts, apps and the like.	Group discussion in class + overview with do's	

Contents per step	Methodology	Media
Question: Can you think of a strong password in your head? **Explanation: Two-Step Verification:** Facebook and Instagram platforms take things a step further to reduce security risks, thanks to two-step authentication. It sounds more complicated than it really is. **Example using Facebook** **1.** Log in to Facebook and click on the arrow at the top right **2.** Now select 'Settings' and then 'Security and login' **3.** Click on 'Edit' in 'Two-factor authentication' and then 'Get started'. **4.** Checkmark 'Text message' to receive the security code on your mobile and click 'Next' **5.** You will receive a code on the phone number you entered. Enter it here. Click 'Next'. The two-step authentication is active. Each time you or someone else logs in from an unknown smartphone or computer, you'll receive a code.	Group discussion in class + overview with do's	Appendices 3, 4, 5, 6 and 7

Deel 5: Being Safe Online

Short description

In the online world, children are confronted with people who do not respect their boundaries, who are mean or even ask for money. It is important to make this debatable and to give children ways to deal with it.
In this part of the lesson, we want to create awareness of assertive online behavior among pupils and provide them with tools to raise the subject of cyberbullying.

Step-by-step

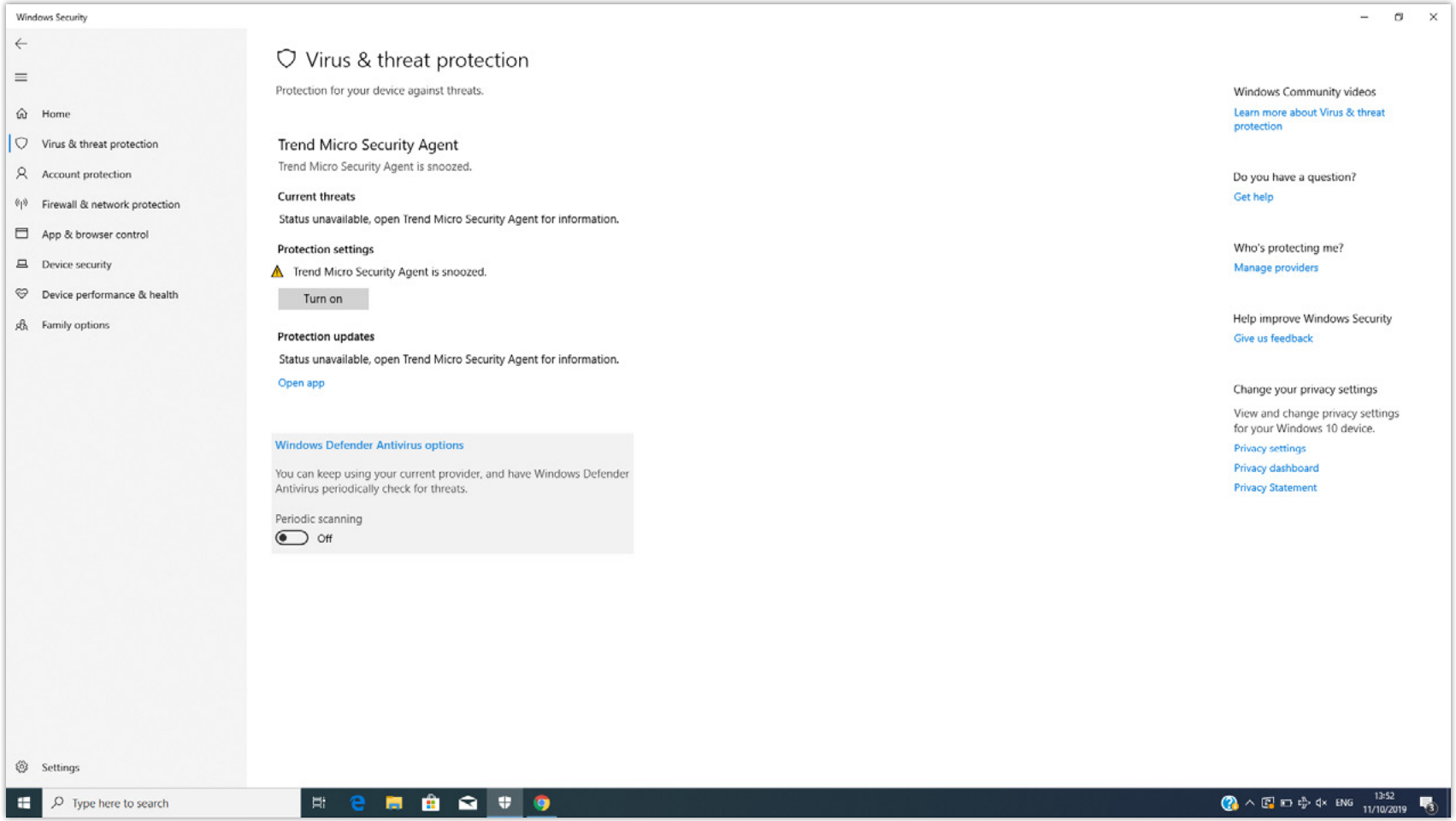
Contents per step	Methodology	Media
Question: In movies like Batman and Superman, it's all about the good and the bad guy. Good against evil. What is good for you on the Internet and what is evil? **Explanation:** Online, you don't owe anything to anyone, even if you've added him or her as a friend to your social media. When in doubt, always check with someone you trust, like your parents or your teacher.	Classroom discussion + classroom teaching	

Contents per step	Methodology	Media
Tips: **1.** Do not send inappropriate photos or videos when someone asks you to (including someone you know very well) **2.** Beware of false information (also called 'fake news') **3.** Always use your common sense when reading something that looks incredible on social media or in an e-mail **Important take-away:** If it looks too good to be true, it usually is.		
Question: What is your definition of cyberbullying?	Work in groups	
Task: Surf to Child Focus's site and find out how to report cyberbullying	Computer work in groups 1 group presents, the other groups can complement	

Contents per step	Methodology	Media
Explanation: There are several ways to report cyberbullying: **1.** You will find someone who listens and can be trusted at the Child Focus helpline: via their website, by telephone at the toll-free number 116000, by e-mail or via Facebook. **2.** On the website awel.be, you can send an e-mail or chat with someone. You can also call them at the toll-free number 102. **3.** You can react on the social media platform itself. On Facebook, for example, you can not only report bullying, but also call on the help of a parent, friend or teacher.	Classroom teaching	Appendices 8, 9 and 10

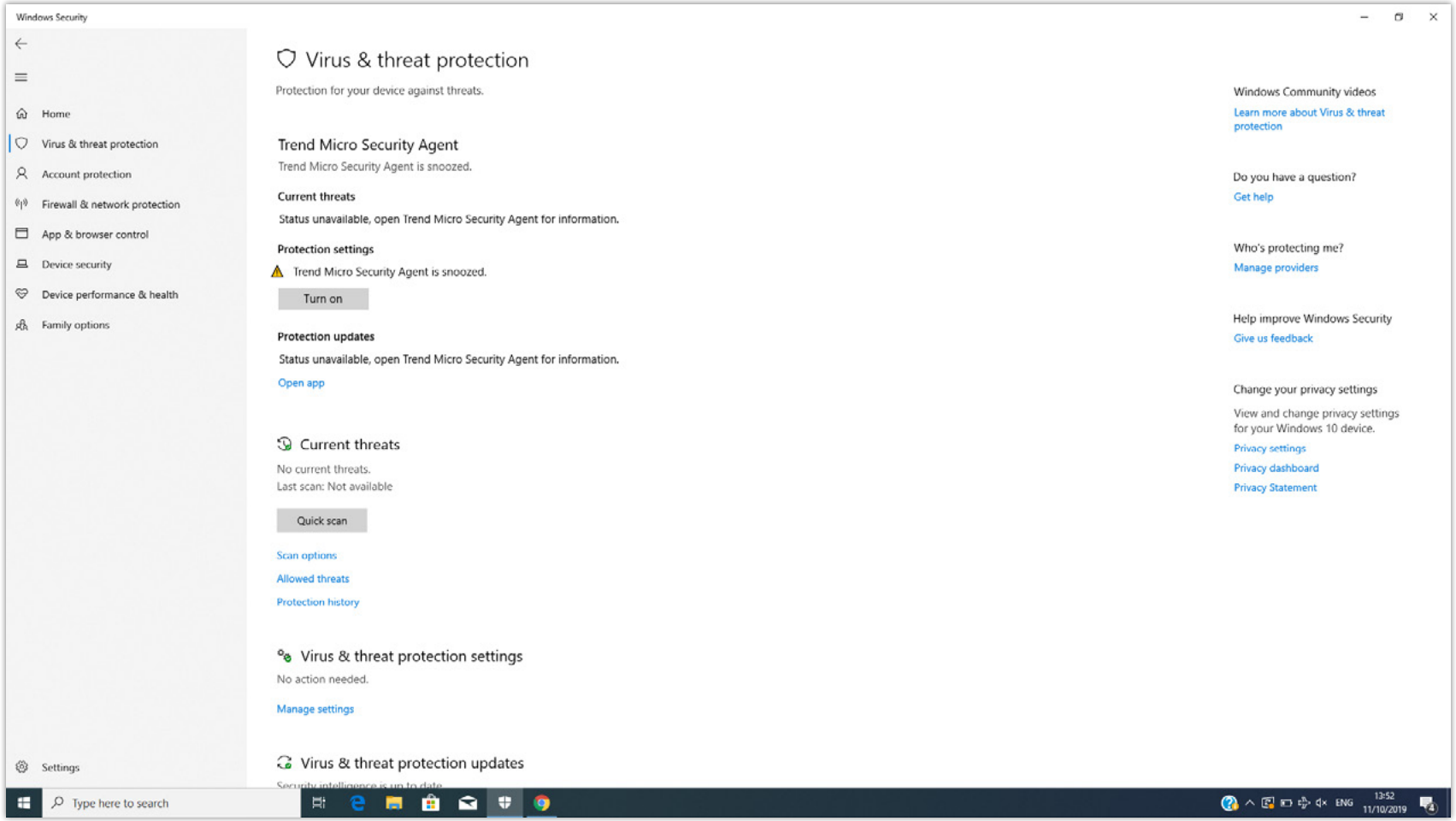
Appendices

1.



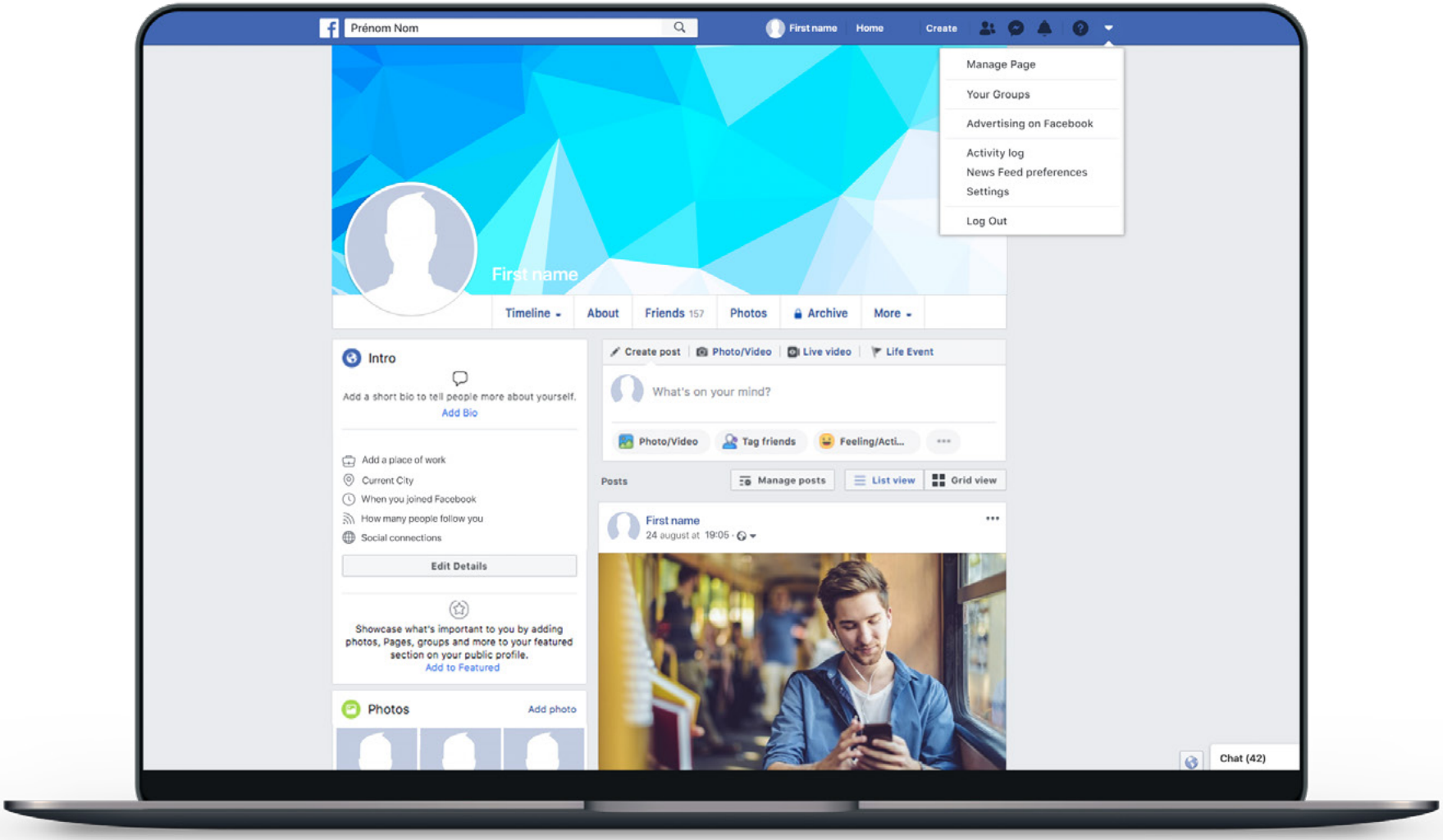
Appendices

2.



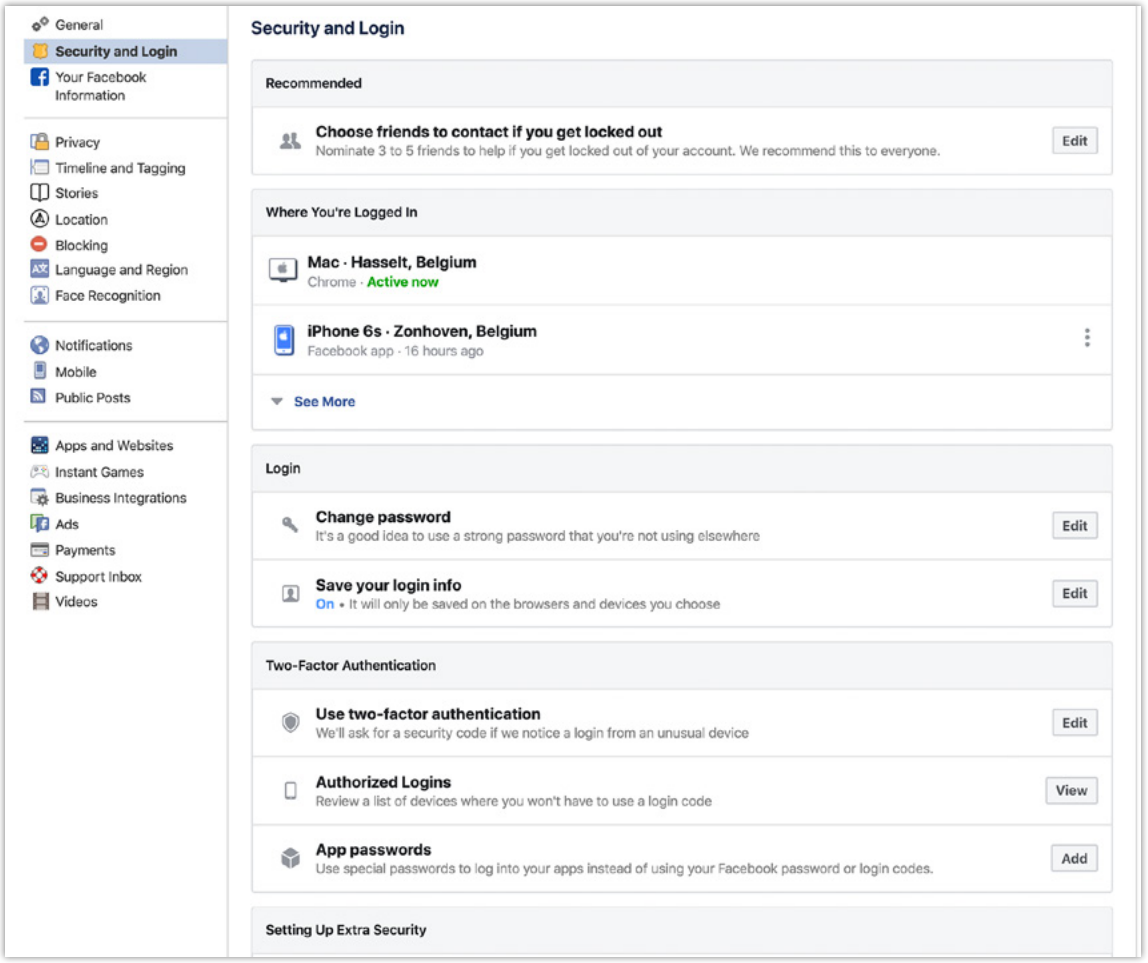
Appendices

3.



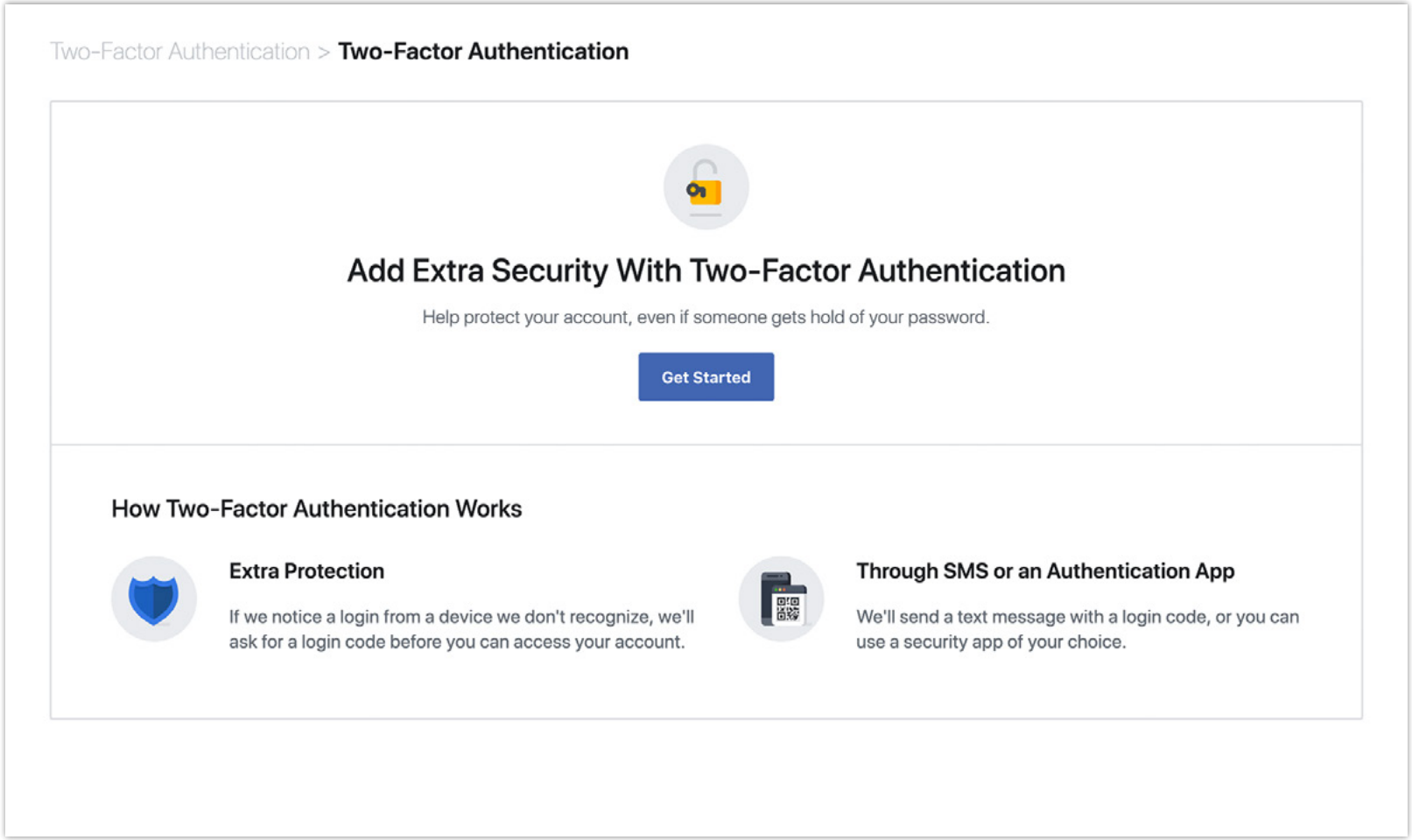
Appendices

4.



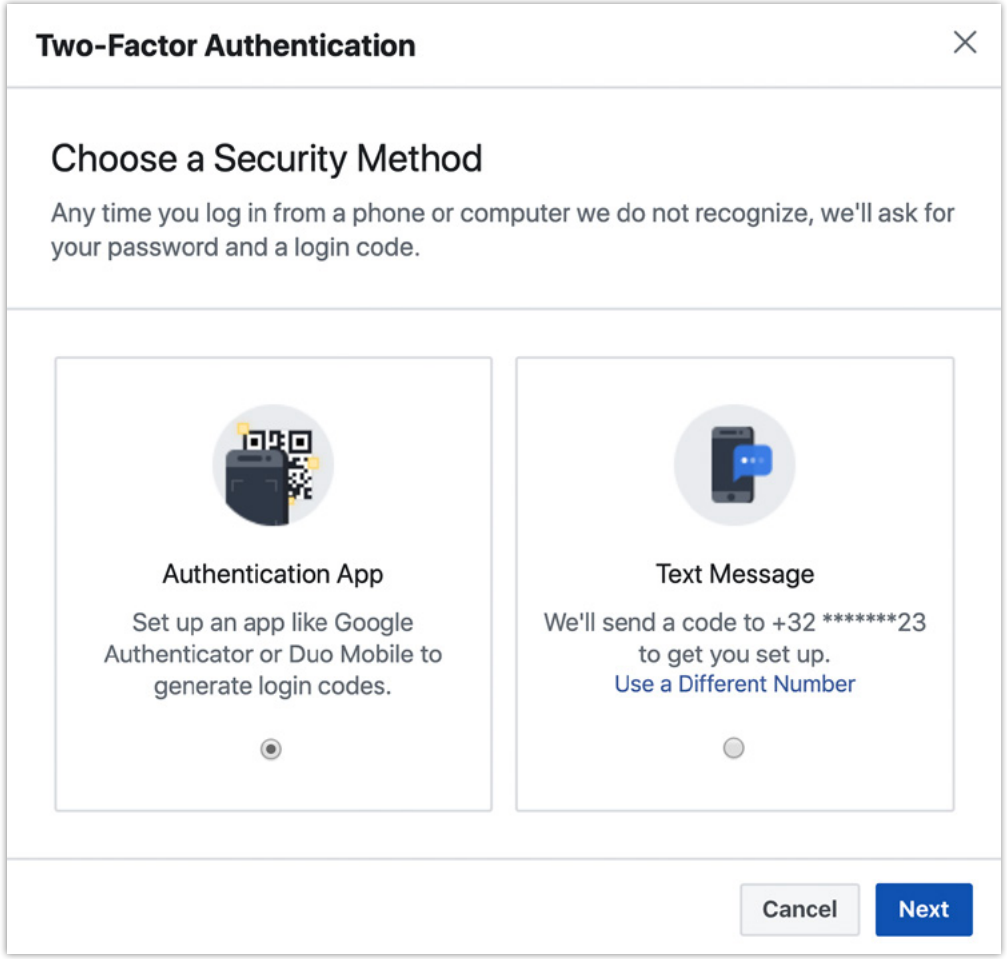
Appendices

5.



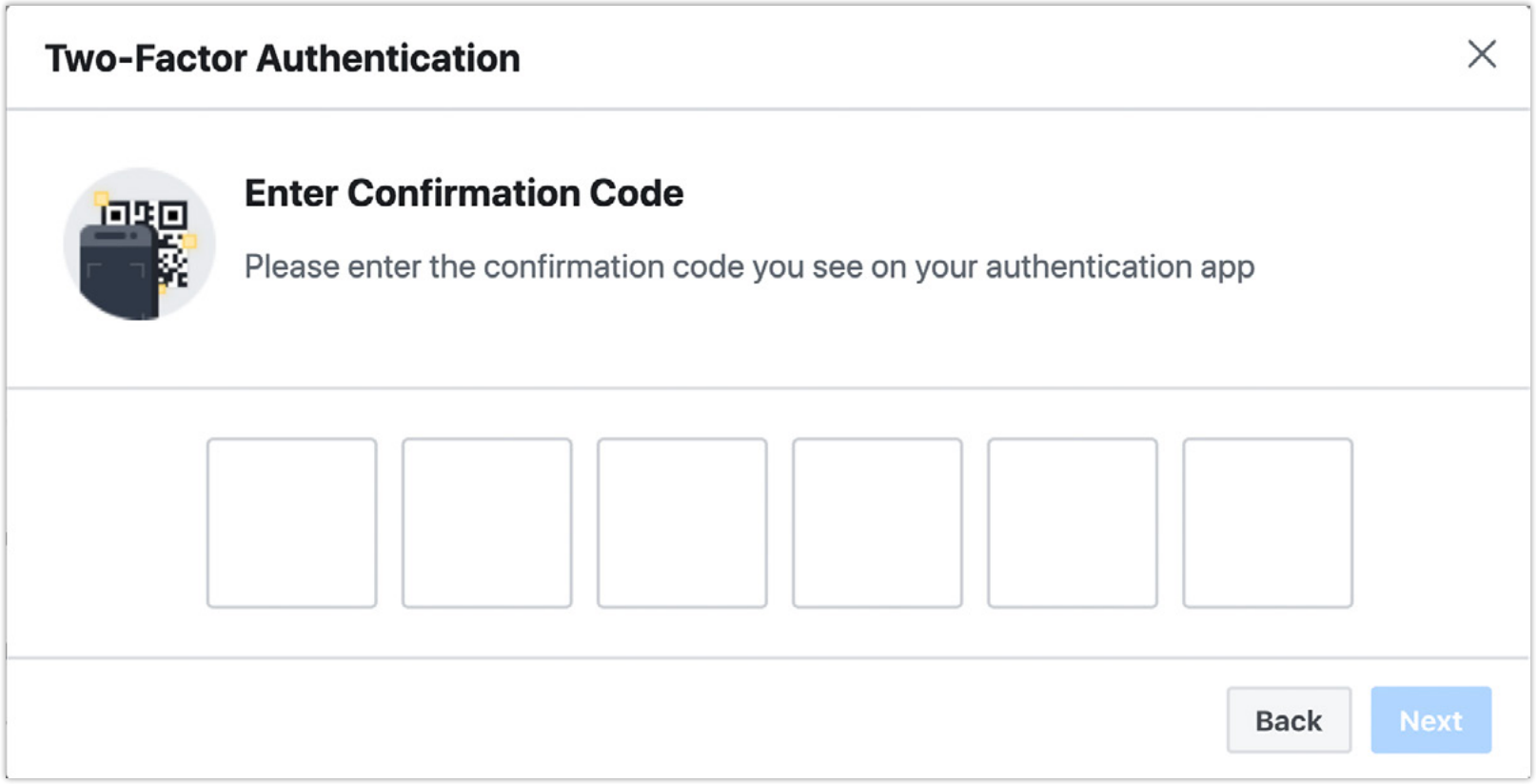
Appendices

6.



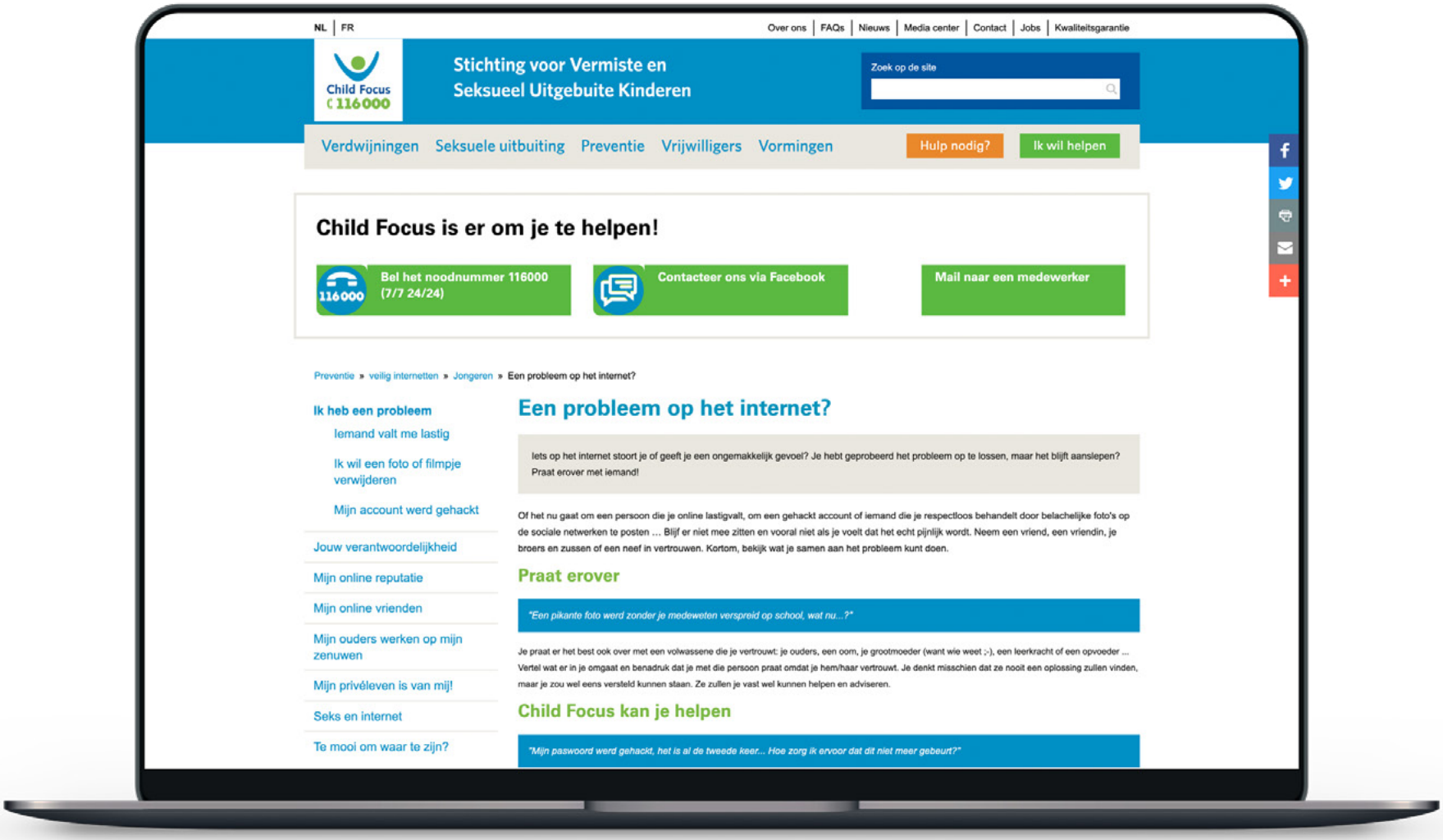
Appendices

7.



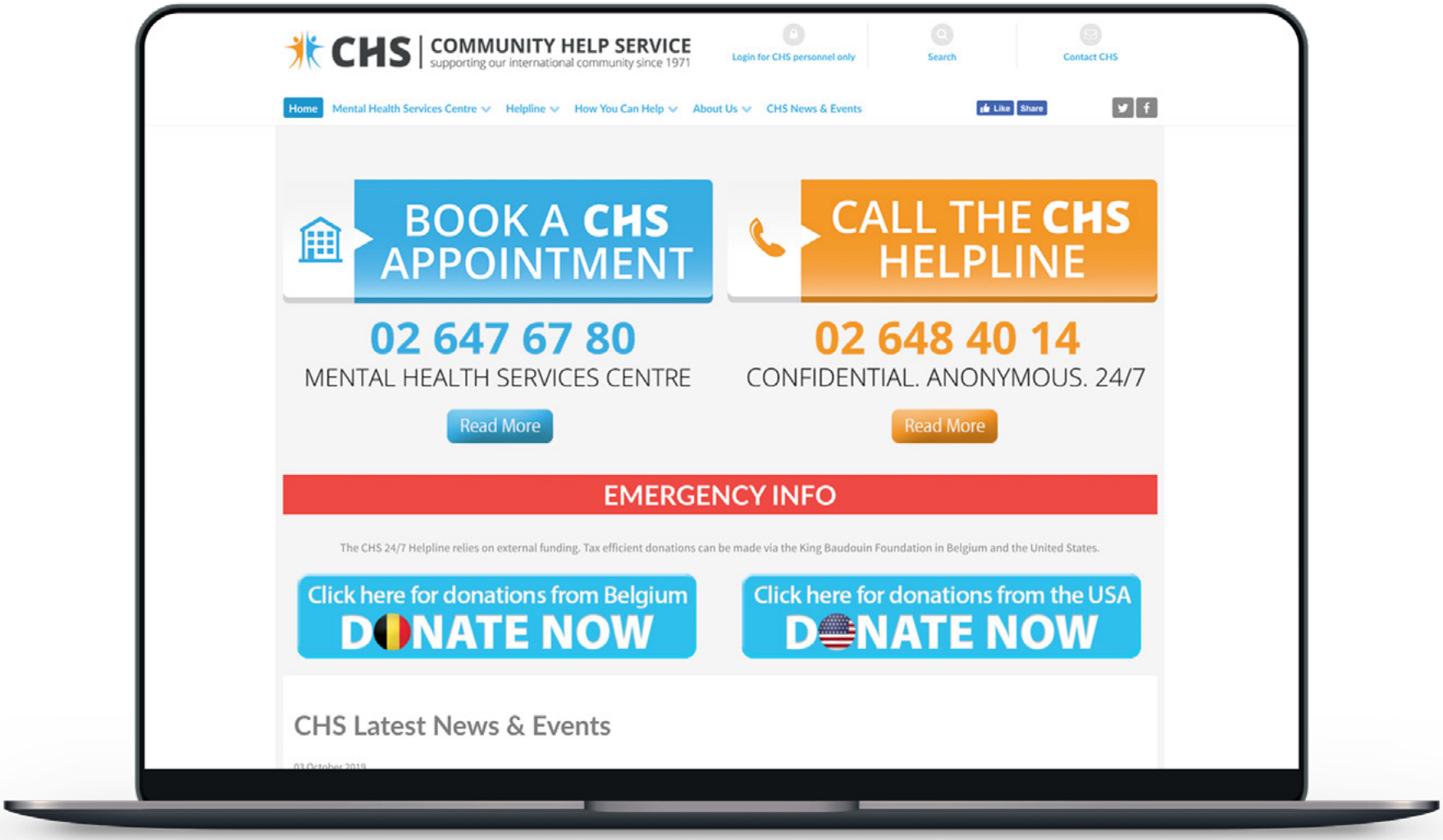
Appendices

8.



Appendices

9.



Appendices

10.