
Hello and welcome!

## Working from home can be a challenge!

CYBER SECURITY COALITION.be

### Recognise this?

BBC interview from home with a little help from the children...


2

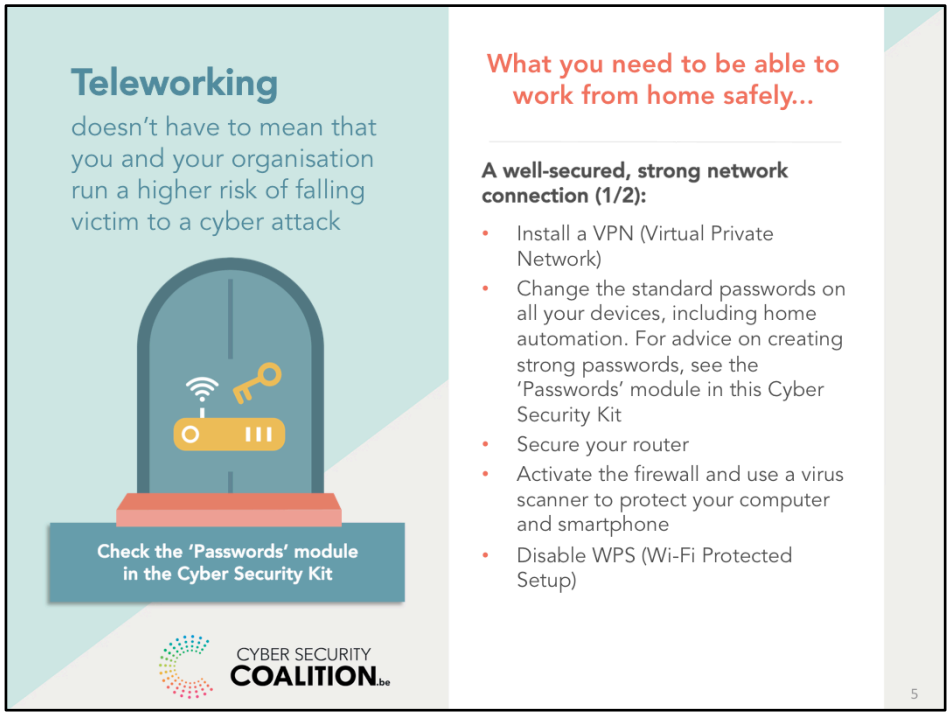
Safe homeworking

**Once upon a time, there was a peacful kingdom**

That brought happiness to all Teleworkers

3


Download verified apps
Protect your home network
Set-up anti-virus software
Ensure wifi is secure
Protect your router
Keep private and work tools separate
4



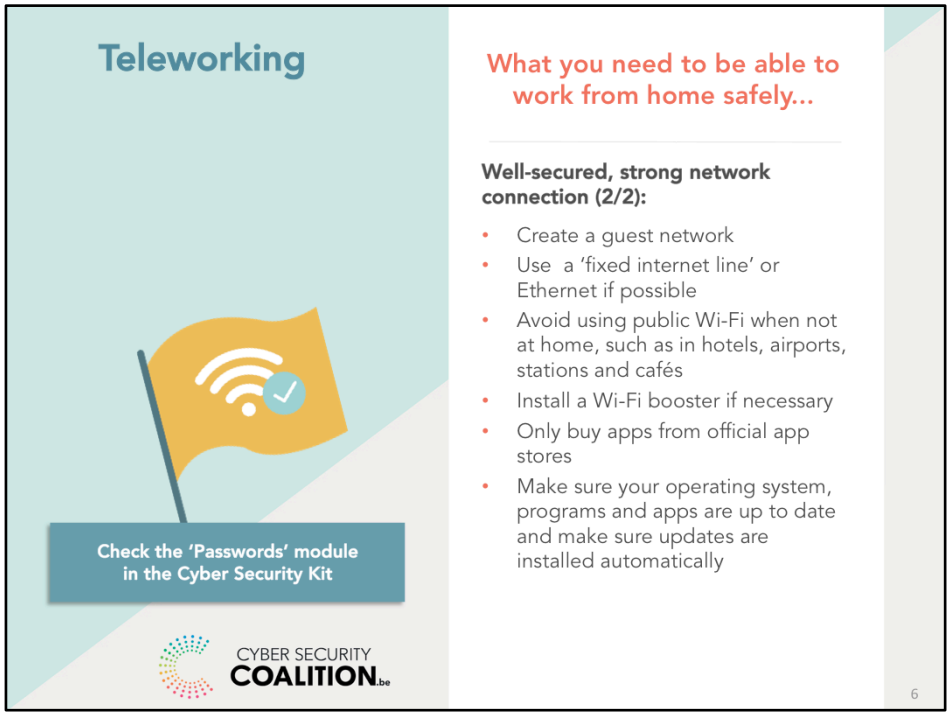

*(Sources: www.safeonweb.be, Vrije Universiteit Brussel, BNP Paribas Fortis, US Department of Homeland Security)*

We use the internet on our smartphones, tablets and computers – and, increasingly, on 'smart' devices such as cameras, TVs and home automation solutions – every day. Yet being dependent on the internet like this involves risk. How can I protect my home network against unwanted users?

Having a well-secured network means:

- Installing a **Virtual Private Network** (VPN). This is your personal **secure tunnel through your Wi-Fi network**. All communication takes place through an encrypted virtual tunnel, stopping cyber criminals from intercepting readable communications and being able to gain access to your information. Many employers provide their employees with a reliable VPN connection allowing them to access their professional network safely. If your employer doesn't, you can install a free or payable VPN service online yourself. A number of virus scanners, for example, offer a VPN.

- Change the standard passwords on **all** of your devices connected to your home network. These may be computers, smartphones, tablets and printers, as well as things like cameras and network systems that easily connect with one another through your home network. Examples of weak standard passwords that are unfortunately still very common are things like 'Admin' and 'password'. For advice on creating strong passwords, see the 'Passwords' module in this Cyber Security

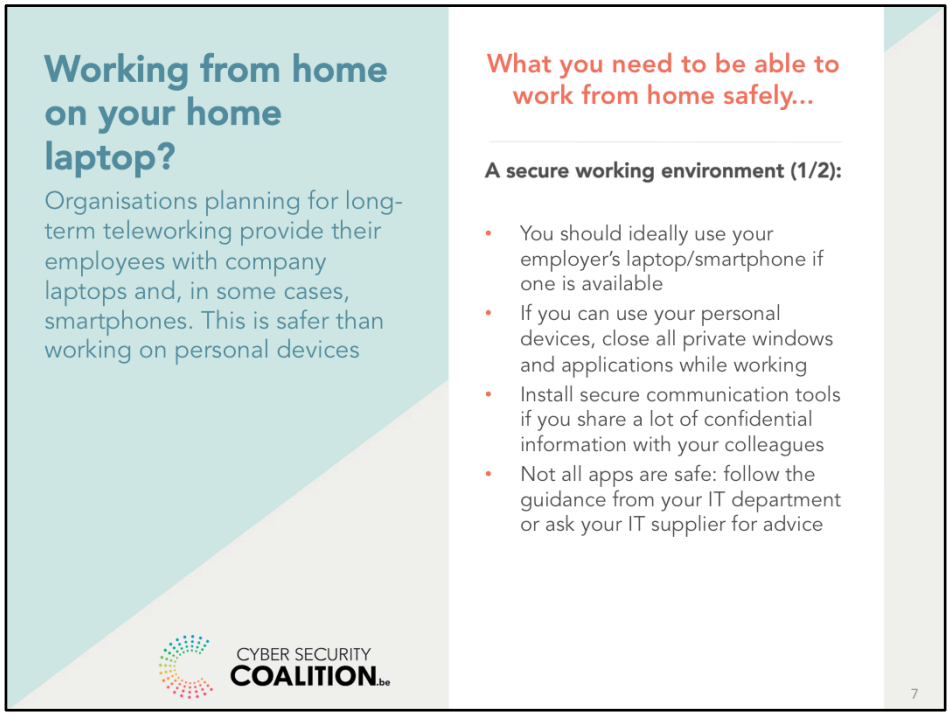



*(Sources: www.safeonweb.be, Vrije Universiteit Brussel, BNP Paribas Fortis, US Department of Homeland Security)*

- **Create a guest network.** A guest network is a separate Wi-Fi network that is strictly separate from your own network. While it allows your guests to access your internet connection, it doesn't allow access to your shared files and devices such as printers and network hard drives. This means you can share your guest network password without having to worry about it. Many routers offer this option in the settings. Make your network even safer by only connecting 'smart' IoT devices (Internet of Things – devices such as lamps, thermostats, etc. connected to the internet that can be operated remotely) to the guest network. This makes it harder for hackers abusing an IoT breach to access your entire network.

- **Use a 'fixed internet line' or Ethernet**. Use an Ethernet cable rather than Wi-Fi for devices that you don't move around, such as desktop computers, TVs and printers. Even secured wireless networks can be cracked by people within range. Wi-Fi sends out and receives radio signals over a fairly wide range, which poses a potential security risk. It is far more difficult for hackers to intercept information sent through cables, as this requires physical access.

- **Avoid using public Wi-Fi** when not at home, such as in hotels, airports, stations and cafés.



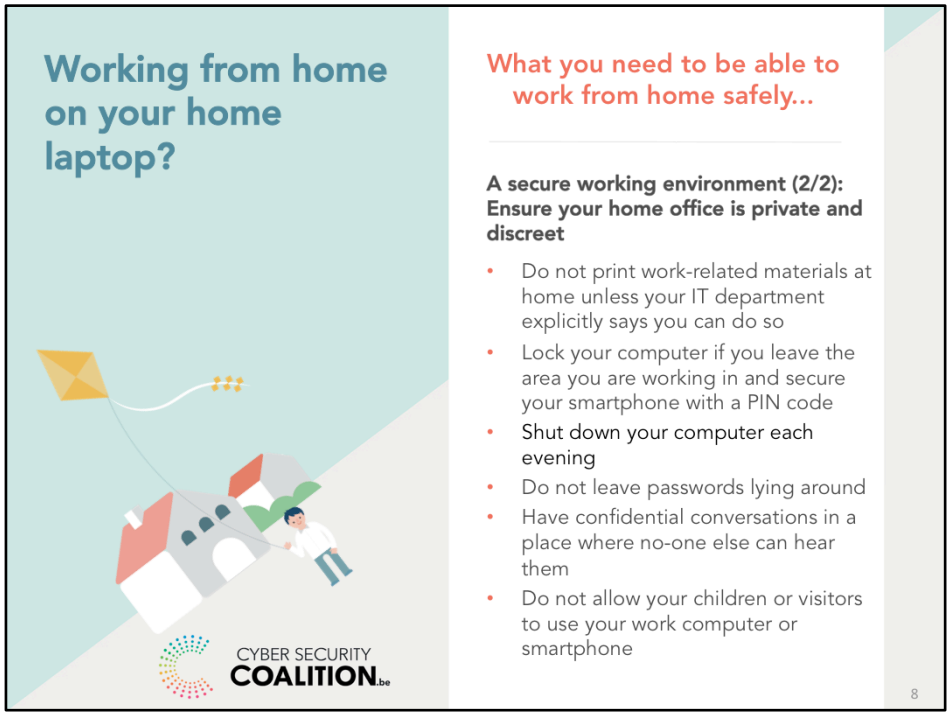

*(Sources: www.safeonweb.be, Vrije Universiteit Brussel, US Department of Homeland Security & BNP Paribas Fortis)*

- You should ideally use your employer's laptop/smartphone. These are **more secure and better monitored** than your own devices. Your employer can also **take immediate action** if a problem arises. Your employer's devices will usually have active antivirus software and update automatically. Employees don't always notice this. When it comes to your personal devices, you're responsible for antivirus software and updates yourself – which you may forget.

- If you can use your personal devices, follow your employer's instructions **and close all private windows and applications while working.**

- **Install secure communication tools (follow guidance from your IT department or ask your IT supplier for advice) if you share a lot of confidential information with your colleagues.** Employees often use WhatsApp to send messages. Services like Threema and Telegram are less well-known alternatives, but are more secure. When it comes to video calls, there are alternatives to Skype, for example (such as Zoom, Teams, Webex, etc.). Read the NVISO advice on Zoom: To Zoom or not to Zoom

- **Not all apps are safe: follow the guidance from your IT department or ask your IT supplier for advice.** If your IT department offers to share confidential information by WhatsApp, for example, or send large files using WeTransfer,




*(Sources: www.safeonweb.be, Vrije Universiteit Brussel & BNP Paribas Fortis)*

A secure working environment means making sure your home office is private and discreet. Specifically, this might mean:

- **Not printing work-related materials at home** unless your IT department explicitly says you can do so.

- **Locking your computer if you leave the area you work in:** Whether at home or in the office, locking your computer if you leave the area you work in is a good habit to get into, so nobody gets the chance to snoop on your files. When there are children around playing or curious teenagers – or even a cat who likes to stand on your keyboard – locking your device when you're not in front of it is always sensible. Locking your device is easy: use the key combination WIN+L, or Ctrl+Shift+Power if you use a Mac. Activating a PIN lock on your smartphone.

- **Shutting down your computer each evening.** Resist the temptation to leave your computer on sleep mode at night so you can get working more quickly the next morning. New updates are installed on your computer when you turn it off. Some of these updates improve security, so it's important for your device to receive regular updates.

- **Not leaving passwords lying around:** Everyone knows you shouldn't stick a post-it with your password on it to your screen. Leaving a discreet slip of paper under


*(Sources: www.safeonweb.be & BNP Paribas Fortis)*

**Spot fake messages quickly**

Pay close attention to the e-mails you receive. The cure for coronavirus isn't going to come by e-mail. The Centre for Cybersecurity Belgium (CCB) is currently receiving a number of reports concerning fake messages about coronavirus on the following topics:

- Offering face coverings
- Fundraising for victims of the virus
- Links to fake news sites
- Offering vaccinations

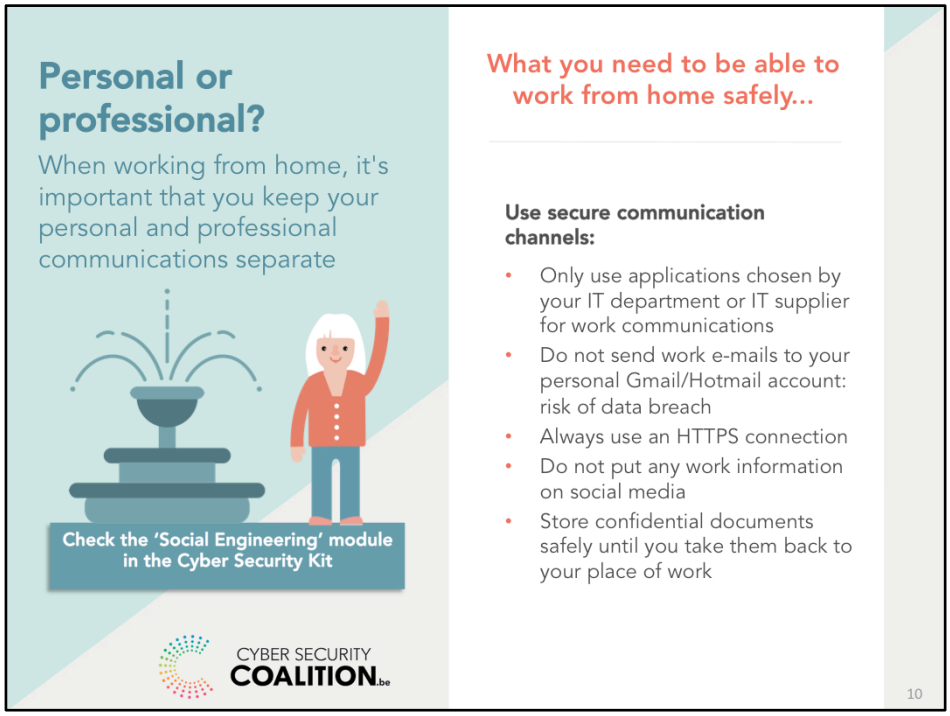
Seek out accurate information. Official reports from FPS Public Health can be found at info-coronavirus.be.

**What should I do if I get a fake message?**

- Do not click on links or images in fake messages and do not open attachments. Only **download attachments or open links** in e-mails from **known, trusted sources.** Do not download attachments or open links from other sources even if the message seems to be urgent or tempting**.**
- If you're unsure, use a search engine to search for the website.
- Never open documents and attachments from unconfirmed official sources about Covid-19 on any device.
- Do not download unofficial software to your computer or apps to your smartphone that do not come from the official App Store to learn more about Covid-19.
- Help prevent the spread of fake messages that might worry your friends or family.
- **Forward suspicious messages to** verdacht@safeonweb.be or your bank's phishing mailbox.

**What should I do if I click on a link or attachment in a suspicious message?**

If you suspect someone knows your password or you have received phishing e-mails or calls to your work e-mail address or phone, have clicked on a link or attachment in a suspicious message, or your work laptop, smartphone or tablet have been lost or stolen, inform your employer immediately.




*(Sources: Vrije Universiteit Brussel & BNP Paribas Fortis)*

**Use secure communication channels**

- Use **applications chosen by your IT department or IT supplier for work communications**.

Communication tools are important when working from home. Your employer's VPN (see slide 4) allows you to connect to your employer's network from home. However, there are a lot of other communication tools out there. It is essential that you clearly separate your personal and work communications and never combine them. You should only use applications chosen by your employer for work communications. Use recognised products from an official app store and make sure they're up to date.

- Do not send work e-mails to your personal Gmail/Hotmail account: **risk of data breach**.

If you're sending an e-mail for work purposes, only use your work account. Sometimes quickly sending a file to your own Gmail/Hotmail account so you can print it at home seems convenient. Bear in mind, though, that this can cause work-related sensitive information to be leaked. Your home printer will not always meet your employer's security requirements, so never do this! Be very cautious when communicating and exchanging information externally. Only use approved solutions.

- Always use an **HTTPS** connection.

When visiting websites, make sure your browser **always uses an HTTPS connection rather than an HTTP connection**. This is especially important if you have to enter personal data such as your username and password. HTTPS uses encrypted, secure communication. The same cannot always be said of HTTP connections, which send your information intact and unencrypted over the internet and which can therefore be intercepted by cyber criminals.

- **Do not put any work information on social media**.

When working from home, the boundary between using your personal social media and work activities is less obvious than it is in the office. Posting little details about your work or daily routine online might seem normal if there aren't any colleagues around to share things with, so when you're working from home, be careful. Updates like these provide valuable information for phishing campaigns.

- Store **confidential documents** safely until you take them back to your place of work. Don't just throw them in with your domestic recycling. In many cases, at work these documents may be discreetly destroyed or processed.


*(Sources: www.safeonweb.be & US Department of Homeland Security)*

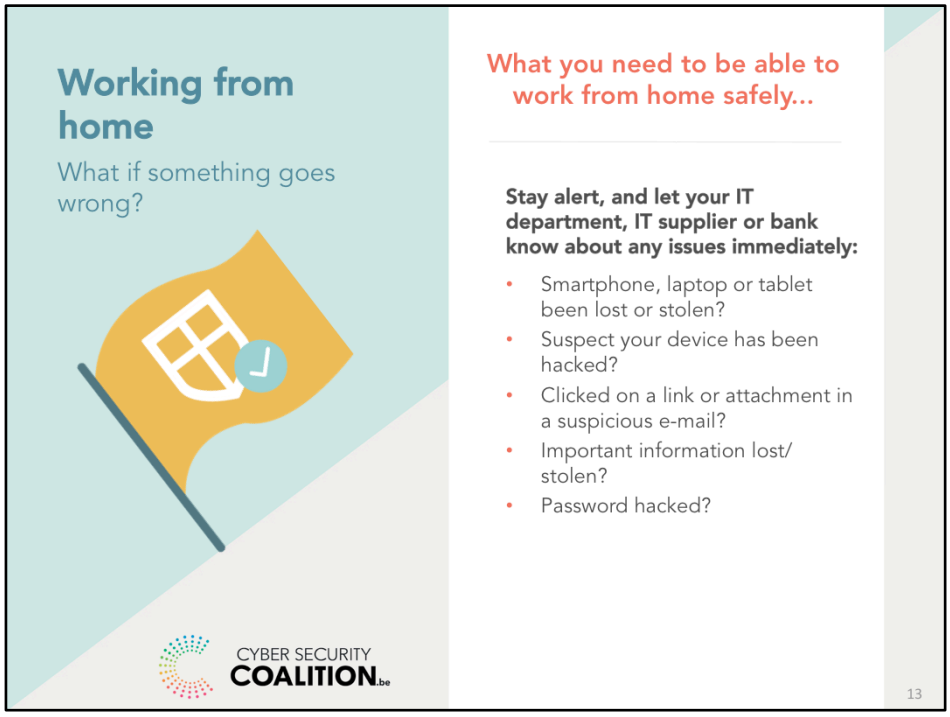
**Hosting online video conferences safely:**

- Use recognised products from an official app store and make sure they're up to date.
    - If you download an app from an app store, only use the **official app stores** (App Store/Google Play).
    - Whatever platform you're using, make sure you always carry out **updates**. Updates provide additional features and resolve bugs. Updates also help to solve security flaws. It's therefore important to install updates every time you're asked to do so.
- Create your **own account** and use a **strong password** to secure it.
- Keep your telephone and video calls **confidential**.
    - Have video calls **in places you can talk without being interrupted**. If you have your meeting on your terrace, your neighbours could hear every word – not something you want. The same is true of trains or other public areas.
    - Watch out for your **'visual' and 'audio' home environment**: don't give away any sensitive information. Use facilities that let you replace your background or blur it.
    - **Only share the meeting link with the people invited**, not in public (e.g. Facebook). This stops uninvited guests appearing. Make sure the host can mute everyone's microphones (disable them), and do so at the start of the meeting, and that the host can determine who can share their screen.
    - **Make all meetings password-protected**. Use the waiting room function to control guest access. If you're the host, make sure you're the first one in the meeting – don't grant other participants access before you.
    - 'Lock' the event once all of the attendees have arrived to stop intruders entering.
    - Use your **headphones** and turn off any security cameras in your home.
    - **Use a webcam cover**. Make sure your webcam is always covered when you're not using it.
    - Ensure your **data is well protected**:
        - You may need extra security if sharing very sensitive data. For more information, look at **specifications and settings**.
        - Ask your employer to create **secure communication channels** if you share a lot of confidential information with colleagues.
    - If you **share your screen or files, or record a meeting**: make sure you do it in a controlled way. Know who else is watching or listening. Be careful if sharing your full screen or individual application.
    - Think about how sensitive the information is before sharing your screen. **Do not discuss any information you wouldn't share by phone**.


*(Sources: www.safeonweb.be & US Department of Homeland Security)*

**Hosting online video conferences safely:**

- Ensure your **data is well protected**.
  - You may need extra security if sharing very sensitive information. For more information, look at **specifications and settings**.
  - Ask your employer to create **secure communication channels** if you share a lot of confidential information with colleagues.
- If you **share your screen or files, or record a meeting**: make sure you do it in a controlled way. Know who else is watching or listening. Be careful if sharing your full screen or individual application.
- Think about how sensitive the information is before sharing your screen. **Do not discuss any information you wouldn't share by phone**.




**Stay alert and let your employer know about any issues immediately:**

- Smartphone, laptop or tablet lost or stolen?
- Suspicious message?
- Clicked on a link or attachment in a suspicious e-mail?
- Important information lost/stolen?
- Password hacked?

Flag any suspicious messages to verdacht@safeonweb.be as well. The CCB will block links to malicious websites to stop you and everyone else falling victim. If a suspicious message appears to come from your bank, you should also send it to your bank's phishing mailbox.

Test your home working safety!

## Test your digital health

test on www.safeonweb.be

CYBER SECURITY COALITION

14


What do you think?

Any comments?

What do you remember?

What will be the first action you take after this presentation?

# Working from home

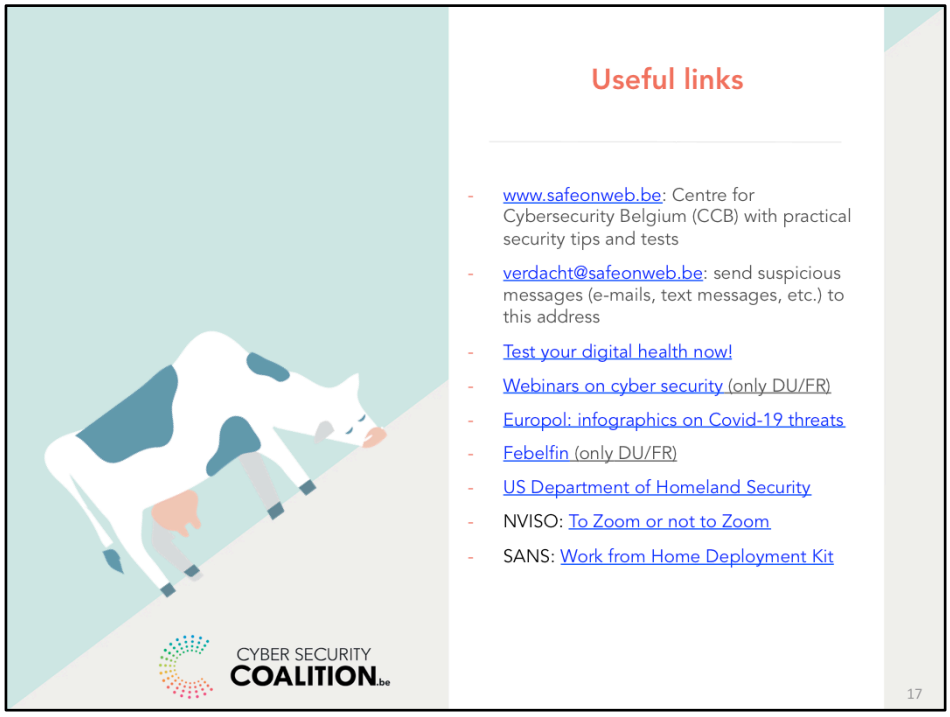
Focus areas

CYBER SECURITY COALITION.be

## SANS focus areas

SANS, a major international cyber security body, has posted this video that offers a serious but accessible overview of the most important messages from these slides:


16




**Useful links:**

**Centre for Cybersecurity Belgium (CCB):**

**-www.safeonweb.be: the Centre for Cybersecurity Belgium (CCB) website, with practical security tips and tests.**

**-suspicious@safeonweb.be: send suspicious messages (e-mails, text messages, etc.) to this address. The CCB can take suspicious links offline.**

-Test your digital health now!: Take the test and see whether your digital health needs a bit of a boost. You'll be asked 15 questions about updates, back-ups, phishing, virus scans and passwords.

-Webinars on cyber security (DU/FR): These webinars can raise organisations' awareness of the most significant cyber threats and offer practical advice on protecting yourself and your customers' information. These webinars are aimed at informing management and all employees involved in digital security.

**Europol:**

https://www.europol.europa.eu/staying-safe-during-covid-19-what-you-need-to-know contains four practical infographics on Covid-19:

- You can go outside again, criminals can too
- At home, still spending plenty of time online?
- Children's safety, a priority
- Protect your finances

**Febelfin (only DU/FR)**

**US Department of Homeland Security**

**NVISO:** To Zoom or not to Zoom

**SANS:** Work from Home Deployment Kit


Thank you for your attention!