SAFE SURFING DURING THE BELGIAN GENERAL ELECTION CAMPAIGN

Recommendations for a cybersecure electoral campaign

MARCH 2024

CENTRE FOR CYBERSECURITY BELGIUM

ADIV-SGRS

VSSE veiligheid van de staat
sûreté de l'état

.be

SAFE SURFING DURING THE BELGIAN GENERAL ELECTION CAMPAIGN

Recommendations for a cybersecure electoral campaign

This guide, entitled *Safe surfing during the Belgian general election campaign,* provides recommendations on how to enhance the security of the various digital tools you use on a day-to-day basis.

Elections form the cornerstone of the democratic process. Terrorist groups, criminals or political actors may try to influence the outcome. As a result, political parties and their candidates are a significant potential target. In this context, the European Union Agency for Cybersecurity (ENISA) has highlighted the disruptive effects of chatbots and the manipulation of information by artificial intelligence (AI). It observed approximately 2,580 incidents, many of them targeting public administrations, between July 2022 and June 2023.

This guide aims to provide you with all the information you need to improve your cybersecurity, limit the associated risks and reduce your digital vulnerabilities.

Most of these tips and tricks will probably seem obvious to you and you might indeed already be applying them. If not, this document will help you to step up the protection of your interests and of your digital security. Furthermore, it is essential that those around you also do all they can to protect themselves. So share these tips and tricks with your family and friends!

The guide *Safe surfing during the Belgian general election campaign* is an initiative of Belgian State Security (VSSE), the Centre for Cybersecurity Belgium (CCB) and the General Intelligence and Security Service (GISS). Each of these bodies contributed its own expertise to the development of this guide.

Brussels, March 2024
Best regards,

Miguel DE BRUYCKER
Director General of the Centre for
Cybersecurity Belgium

Francisca BOSTYN
Administrator General a.i.
of Belgian State Security

Stéphane DUTRON
Major General, Head of the
General Intelligence and
Security Service

[1] ENISA Threat Landscape 2023, *Impact of social engineering & information manipulation campaigns.* See also Chapter 4 'Addressing FIMI During Electoral Processes' in 2nd EEAS *Report on Foreign Information Manipulation and Interference Threats* (January 2024).

CONTENTS

I CAN IDENTIFY SUSPICIOUS MESSAGES

THE TERM 'PHISHING' REFERS TO ACTS OF ONLINE SCAMMING IN THE FORM OF FAKE E-MAILS, MESSAGES OR WEBSITES. SUCH E-MAILS AND THEIR LINKS AND ATTACHMENTS OFTEN OPEN YOU UP TO A CYBERATTACK. HERE ARE SOME THINGS TO THINK ABOUT BEFORE YOU DECIDE TO CLICK ON A LINK OR AN ATTACHMENT:

> The sender of an e-mail. Do you personally know the sender? Is it their usual e-mail address? Does the e-mail address look legitimate? Does this person or organisation often send me this type of document? If in doubt, call the person or organisation who supposedly sent you the e-mail.

> The nature of the request. Are you being asked for personal or sensitive information? If in doubt, never share any personal or sensitive details.

> The wording of the message. Does the e-mail contain spelling or grammar mistakes? Is the sender trying to make you curious? Are they making promises that seem too good to be true? Are they asking you for money? Is the mail creating a sense of urgency? If in doubt, don't click!

> Don't click on links or QR codes in fraudulent messages or open any attachments! If you're unsure, use a search engine to look up the site.

> Learn how to spot a fake link with the 'Surf without worries' online training module: https://surfwithoutworries.safeonweb.be/en/modules/1

> Never give your personal details.

> Forward suspicious messages to suspicious@safeonweb.be

> Install the Safeonweb browser extension. The Safeonweb extension is a tool allowing you to assess the *bona fide* nature of a website. The Safeonweb browser extension will tell you for each website you visit whether the owner has been validated (green) or not (amber).

More information:

- https://safeonweb.be/en/learn-identify-fake-e-mails
- https://surfwithoutworries.safeonweb.be/en/modules/1

I PROTECT MY ACCOUNTS AND USE TWO-FACTOR AUTHENTICATION (2FA)

TAKE GREAT CARE WHEN CHOOSING PASSWORDS. PASSWORDS ARE ALWAYS NEEDED TO PROTECT YOUR DEVICES, DATA, NETWORKS (E.G. WI-FI) AND ACCOUNTS (E.G. E-MAIL OR SOCIAL MEDIA). HOWEVER, EVEN THE STRONGEST PASSWORD ISN'T A GUARANTEE OF COMPLETE SECURITY.

Two-factor authentication improves the level of security when accessing your accounts and devices. Even if a cybercriminal manages to get hold of your password, they will be unable to access your accounts if they can't get beyond other layers of security.

> Use two-factor authentication (2FA) whenever possible. Most of the services offered by major digital platforms (such as social media) as well as a lot of equipment provide this possibility (e.g. via fingerprint and/or facial recognition).

> Use multiple passwords. It is safest to use a different password for each sensitive service (your bank, e-mail, social media, etc.). That way, if one of your passwords were to be compromised, only one service would be affected.

> Long and original. The longer your password is, the stronger it will be. Avoid using a single word that appears in the dictionary. Instead, go for combinations of multiple words that have no apparent connection between them but are easy to remember.

> You can choose to use a password manager. This is a secure program that manages all your passwords.

> No trace. Don't put your password on a Post-it note next to your computer, in an e-mail or in a file on your computer.

> Don't share your passwords or accounts with third parties. By sharing your accounts with others, you may well dilute responsibility for the accounts in question and so make steps taken in the user's name less traceable.

Meer informatie:

- https://safeonweb.be/en/use-strong-passwords
- https://safeonweb.be/en/use-two-factor-authentication
- https://atwork.safeonweb.be/MFA

I ENSURE THAT MY DEVICES AND PROGRAMS ARE OFFICIAL AND UP TO DATE

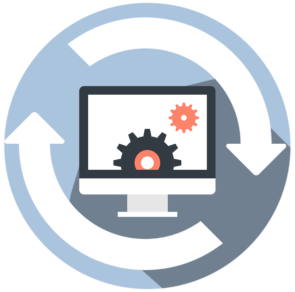
STOP CYBERCRIMINALS OR OTHER HACKERS ACCESSING YOUR DEVICE OR DATA BY INSTALLING REGULAR SECURITY UPDATES, BOTH FOR YOUR OPERATING SYSTEMS AND FOR YOUR PROGRAMS AND APPS. ALL PROGRAMS CONTAIN SO-CALLED VULNERABILITIES, WHICH MAKE IT POSSIBLE FOR CYBERCRIMINALS TO CAUSE YOU HARM OR TAKE CONTROL OF YOUR DEVICE. THESE VULNERABILITIES ARE DETECTED AND RESOLVED WHEN YOU INSTALL AN UPDATE.

> **Enable automatic updates of your devices and software.** This helps ensure that your device is better protected when a vulnerability is detected.

> **Only use official sites.** If you need to download software or a software update, only do so from the manufacturer's official website.

> **Only install secure apps and programs.** Install apps from a standard app store (Google Play, App Store) and programs from an official vendor. Only allow your apps to access strictly necessary information. For example, there is no need whatsoever for a calculator app to have access to your location or contacts. Regularly check the data your apps use in order to detect any illicit traffic.

> **Don't bypass your device's default security system** (by making use of jailbreaking[2] or routing[3], for example). While this might make you feel more in control of your device while still having access to security features, it dramatically increases the risks.



> **Switch off your device each day.** This is because updates are generally installed automatically when the device starts up.

More information on updates:

- https://safeonweb.be/en/do-regular-updates
- https://atwork.safeonweb.be/tools-resources/how-manage-updates

[2] Jailbreaking means enabling an iPhone, iPod touch, iPad or Apple TV to load software applications that are not recognised by Apple.

[3] Routing a smartphone or tablet involves making a software update with a view to accessing the device's administrator account which has access to all the features and settings.

I ENSURE THAT MY DEVICES ARE PROPERLY PROTECTED

IF ONE OF YOUR DEVICES ENDS UP IN THE WRONG HANDS, YOU COULD BE IN BIG TROUBLE. THEREFORE, BE SURE TO PROTECT YOUR SMARTPHONE, TABLET, LAPTOP, ETC.

> **Proper locking.** Ensure that your smartphone locks automatically when idle (maximum idle time of one minute). Use a code rather than a pattern. If the feature is available, enable a temporary lock on your smartphone that is activated after several incorrect attempts to access the device and deletion of data if too many access attempts are made. Make sure of course that high-quality backups are in place.

> **Encrypt your devices.** If you can, encrypt your devices, as well as your USB drives and external hard drives. If you're using an SD card, encrypt that too.

> **Limit access.** Be sure to only enable access to Wi-Fi, Bluetooth, Near Field Communication[4] (NFC), your data, geolocation, etc. when you need it. Don't activate auto-activation functions (e.g. for Wi-Fi). Check app access rights regularly.

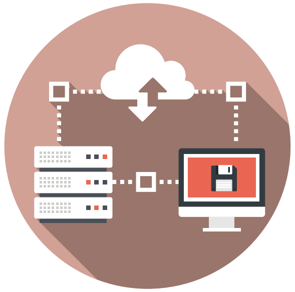
> **Stay in control of your device.** Don't leave it unattended.

[4] Near Field Communication (NFC) is wireless communication allowing exchanges of small volumes of data within a 10-cm radius, for example to make a connection with a payment system or a smartphone.

I ENSURE THAT MY DATA IS PROPERLY PROTECTED

YOU ALSO NEED TO HANDLE THE DATA YOU KEEP ON YOUR COMPUTER WITH CARE. LOSING YOUR DATA ISN'T ONLY ANNOYING TO YOU PERSONALLY BUT IF MALICIOUS ACTORS STEAL AND EXPLOIT YOUR PARTY MEMBERS' DATA, FOR EXAMPLE, THIS CAN ALSO CAUSE A HEADACHE.

> **Make backups.** A backup is an extra copy of data that is important to you. This will allow you to restore the data on your device if you are hit by a virus. It is also reassuring to have a backup in the event of theft, loss or technical problems. You can then reinstall your entire system and restore your data. **This of course also applies to your mobile devices.**



> **Save your data.** Set up a system to regularly save your data automatically. Decentralised (cloud) solutions can really help in this regard as long as yours is a trusted provider.

> **Use a virus scanner.** A virus scanner should mean that your computer won't be infected by viruses. This is the most important piece of software for protecting your computer and data.

> **Switch off.** Switch off your devices when you aren't using them (holidays, weekends, etc.) and disable the functions you aren't using (Wi-Fi, Bluetooth, NFC, geolocation).

> **Be careful when using USB sticks.** While a USB stick is handy for carrying data, it can also be easily lost. Pay particular attention with USB sticks that you receive from other people or that you might find on the ground, for example, as they may contain viruses. We therefore advise you to have a scan carried out (by a professional) for potential viruses before using the USB stick in question. Regularly save the contents of your USB sticks and delete unnecessary documents on them.

More information on backups:

- https://safeonweb.be/en/make-back-ups
- https://atwork.safeonweb.be/tools-resources/how-manage-backups

More information on virus scanning:

- https://safeonweb.be/en/scan-your-computer
- https://atwork.safeonweb.be/tools-resources/antivirus-software

More information on USB sticks:

- https://cyfun.be (Cyber Fundamentals - Small, '3. Install antivirus').

I USE A SECURE (WI-FI) NETWORK

A SECURE NETWORK IS AN ESSENTIAL PRECONDITION FOR HIGH-QUALITY PREVENTION. IF A CYBERCRIMINAL OR ANOTHER HACKER MANAGES TO ACCESS YOUR NETWORK, THEY WILL ALSO HAVE ACCESS TO ALL THE DEVICES CONNECTED TO THAT NETWORK. WI-FI HAS CONSIDERABLY SIMPLIFIED ELECTRONIC DEVICES' CONNECTIONS TO DIFFERENT NETWORKS (INTERNET, PRIVATE NETWORK, CORPORATE NETWORK, ETC.). HOW TO MAKE YOUR WI-FI AS SECURE AS POSSIBLE.

> **Secure your personal router.** When you receive a new Wi-Fi router (or a new Wi-Fi box), change the default settings. Change the network name (SSID), not including anything obvious in that name. Also change the passwords (including the password securing your router).

> **Use WPA2 protection.** Your router will probably have various encryption options (WPA2, WPA, WEP). Select WPA2, installing this immediately if you haven't already done so.

> **Install a firewall.**

> **A strong access code.** When choosing your Wi-Fi network access code, refer to the advice given above for passwords. Only reveal it to people you trust. Change it regularly.

> **Avoid using public Wi-Fi networks.** We recommend that you don't carry out banking or other important transactions on a public Wi-Fi network. Avoid creating password-protected accounts on a public Wi-Fi network.

> **Install a Virtual Private Network (VPN).** This is a personal and secure 'tunnel' using the Wi-Fi network. You can install VPN services online free of charge or for payment. Various virus scanners also offer a VPN.

More information on Wi-Fi:

- https://safeonweb.be/en/news/there-any-wi-fi
- https://atwork.safeonweb.be/tools-resources/protect-your-mobile-devices
- https://atwork.safeonweb.be/tools-resources/how-stay-vigilant-against-cyber-threats

More information on WPA2 security:

- https://cyfun.be (Cyber Fundamentals - Small, '4. Secure your network').

I USE SOCIAL MEDIA WITH CARE

WHEN IT COMES TO PRIVACY, POLITICIANS ARE MORE VULNERABLE THAN OTHER CITIZENS. BEING ACTIVE ON SOCIAL MEDIA MEANS THAT NOT ONLY DO YOU COME INTO CONTACT WITH THE OUTSIDE WORLD BUT THE OUTSIDE WORLD CAN ALSO BUILD UP A PROFILE OF YOU BASED ON THE INFORMATION YOU SHARE, RANGING FROM PERSONAL PHOTOS TO HOW YOU BEHAVE, INCLUDING YOUR FAVOURITE FILMS, WHAT YOU EAT, INFORMATION ABOUT YOUR FAMILY, YOUR NETWORKS AND YOUR LOCATION. AS A RESULT, THIS INFORMATION CAN BE MISUSED.
HERE ARE SOME TIPS TO HELP YOU PROTECT YOUR PRIVACY.

> **Use different devices.** If possible, use different devices for your political or other work on the one hand and your private life on the other.

> **Use several e-mail addresses.** For example, you could use one e-mail address for sensitive services (your bank, public authorities, etc.) and another for services that are less sensitive (video on demand, forums, games, etc.). It would be best to also have an e-mail address that is only for your public-facing work.

> **Consider the security of your social media accounts.** Check the settings of your social media before the campaign (including certain automated posts). Before you post anything, decide who will be able to view your post, based on what you want to share. Enable strong two-factor authentication (2FA) for access to your accounts.

> **Beware of internet trolls.** Their main goal is to provoke, influence, direct and escalate online discussions. They do this by creating social media accounts in advance which look like they belong to ordinary members of the public. When the time comes, they then swing into action to take a standpoint on a particular subject. You can stop the troll in their tracks by not responding the way they want you to. Don't get into a discussion, and keep your cool.

> **Where possible, avoid linking your accounts.** Some platforms allow you to log in with your existing account from other social media. These linked accounts are vulnerable because all your personal data is brought together on a specific platform.

> **The privacy settings for your accounts should be checked regularly.** Settings can sometimes be changed unilaterally by the provider, potentially meaning, for example, that ownership rights to your personal information may be transferred to the platform operator.

> **Note that some social media platforms may have links to specific countries.** For example, TikTok is based in China. Therefore, data stored on this platform may be used or misused by the Chinese government. Consider whether you really do need to have a presence on all the various social media sites.

I CAN IDENTIFY DISINFORMATION

DISINFORMATION POSES A THREAT TO OUR DEMOCRACY BECAUSE IT CAN PREVENT VOTERS FROM MAKING AN INFORMED POLITICAL CHOICE. THIS CAN BE SEEN, IN PARTICULAR, IN THE DISSEMINATION OF FALSE OR MANIPULATED INFORMATION, AND ALSO THE DELIBERATE RAMPING-UP OF DIVISIONS, THE ENCOURAGEMENT OF DISTRUST IN THE ELECTORAL PROCESS OR THE EXCLUSION OF LEGITIMATE VOICES FROM PUBLIC DISCOURSE. AS A POLITICIAN, YOU COULD BE THE TARGET OF DISINFORMATION OR EVEN UNINTENTIONALLY FUEL IT YOURSELF.

> **Learn about disinformation.** Disinformation isn't necessarily the same thing as propaganda or 'fake news'. It can also come in many forms, e.g. not only fake news sites or fake images but also fake audio messages or conspiracy videos on TikTok. The National Crisis Center website explains in detail exactly what disinformation is and the various techniques that are typically used to influence others: https://crisiscenter.be/en/disinformation

> **Use your common sense.** You can recognise misinformation by asking yourself a few questions: Who is the author, creator or disseminator/broadcaster? Is the information true? What was the purpose of creating or posting the message? Other tips: read beyond the headline/subject line, consult multiple sources, check the date when a message was written or posted, and be mindful of the format.

> **Beware of 'deepfakes'.** The rapid rise of generative AI makes it a lot easier to manipulate images or create completely fake photos, videos and audio. Playing a video in slow motion may be the first means of spotting these deepfakes.

> **Check the facts yourself.** To check the accuracy of images, you can also take the following steps: Using a search engine, such as Google Reverse Image Search, you can find the actual context. Look carefully and note the various environmental features that tell you more about the location. Track down independent sources to fact-check stories or images. Further advice can be found at https://belux.edmo.eu/tools/fact-checking-toolkit/

> **Don't share questionable content.** Still have doubts about the accuracy or reliability of a piece of information? Then don't pass on this information or message. Not only is this what the people behind it are hoping for but, as a politician, you have a very substantial sphere of influence and you lend disinformation extra weight by sharing it through your channels.

> **Report the disinformation.** Are you sure you're dealing with disinformation? If you are, you can report it to EDMO BELUX at https://belux.edmo.eu/disinformation-reporting/

I'M A VICTIM: WHAT SHOULD I DO?

1. I'M A VICTIM OF A CYBERATTACK THAT IS STILL GOING ON

> You can limit the consequences of a cyberattack if you take prompt action.

> You can report the incident to the CCB via the form on the CCB website or by e-mail at incident@ccb.belgium.be. You will find more ways to report an incident at https://cert.be/en/report-incident-0

In an emergency, you can also call the CCB on **+32 (0)2 501 05 60.**

> DON'T switch off your computer, otherwise you will erase the traces left by the perpetrators of the cyberattack.

> It is also best to change passwords on a secure computer as the perpetrator may have them in their possession.

> File a report with the local police.

More information:

- https://ccb.belgium.be/en/cert/first-port-call-event-cyberattack

2. MY ACCOUNT HAS BEEN HACKED

> Change all your passwords immediately. To do this, use a secure device, i.e. one that is different from the one from which your data was stolen.

> Add two-factor authentication (2FA) immediately.

> Run a virus scan on your computer.

> If your bank or credit card details have been stolen, notify your bank and monitor your accounts. Call Card Stop on **078 170 170 (+32 78 170 170 from abroad).**

> If data relating to your political activities has been stolen, notify your party as soon as possible and report the theft to the Belgian Data Protection Authority.

> Notify your contacts. After all, they may well receive messages sent fraudulently in your name.

More information:

- https://safeonweb.be/en/my-account-has-been-hacked

3. I'VE LOST MY DEVICE OR IT HAS BEEN STOLEN

> Immediately change all passwords for the accounts that were on your device (e-mail, Facebook, WhatsApp, etc.).

> If your bank details or payment data were on the stolen device, notify your bank via your contact person and monitor your accounts carefully. If necessary, have your bank cards and accounts blocked via Card Stop (www.cardstop.be (in FR and NL) or **078 170 170 (+32 78 170 170 from abroad)**).

> If data relating to your political activities has been stolen, notify your party as soon as possible.

> If your device has been stolen, report this to the police.

More information:

- https://safeonweb.be/en/i-lost-my-smartphone-or-tablet

4. MY DEVICE HAS BEEN INFECTED WITH A VIRUS

> You must get rid of any virus as soon as possible.

> If you don't yet have a virus scanner and your computer isn't locked, then it's time to install one, run a scan and remove the virus. In the meantime, don't enter any personal or payment details, as some viruses may forward this information.

More information:

- https://safeonweb.be/en/help-i-have-virus

RELEVANT CONTACTS

1. **CENTRE FOR CYBERSECURITY BELGIUM (CCB)**

> The CCB is your point of contact for reporting any cyberincidents and asking any questions, both during and after the election.

You can get in touch with the Centre by sending an e-mail to incident@ccb.belgium.be or reporting an incident at https://ccb.belgium.be/en/cert

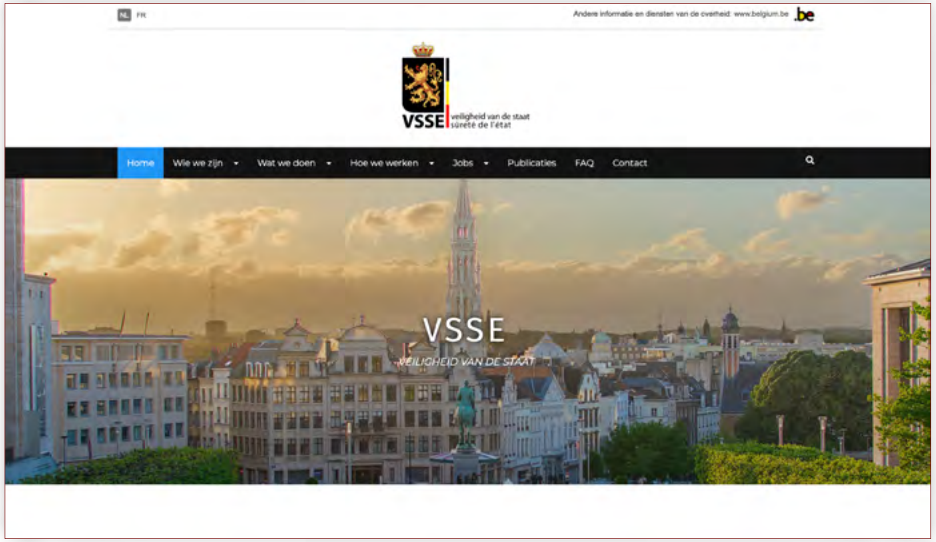
In an emergency, you can also call the CCB on **+32 (0)2 501 05 60.**

2. **BELGIAN STATE SECURITY (VSSE)**

> You will find full information on the missions and operation of the VSSE on its website: www.vsse.be (in FR and NL).

3. **GENERAL INTELLIGENCE AND SECURITY SERVICE (GISS)**

> You can learn more about the role and responsibilities of the GISS by contacting this service at the following address: csoc@cyber.mil.be


NL FR
Andere informatie en diensten van de overheid: www.belgium.be .be
VSSE veiligheid van de staat sûreté de l'état
Home
Wie we zijn
Wat we doen
Hoe we werken
Jobs
Publicaties
FAQ
Contact
VSSE
VEILIGHEID VAN DE STAAT

MORE INFORMATION

CYBERATTACKS:

> **Centre for Cybersecurity Belgium:** https://ccb.belgium.be/en/cert

> **Safeonweb@work:** https://atwork.safeonweb.be/

> **CyberFundamentals:** https://cyfun.be

> **Cyber Security Basics for Starters:**
https://www.cybersecuritycoalition.be/cyber-security-basics-for-starters/

> **Cyberscan (FPS Economy):** https://economie.fgov.be/en/cyberscan

> **Belgian Data Protection Authority:** https://www.dataprotectionauthority.be/

> **Platform for reporting fraud:** https://pointdecontact.belgique.be/meldpunt/en/welcome

> **Safeonweb:** https://safeonweb.be

DISINFORMATION:

> **Disinformation (National Crisis Center):**
https://crisiscenter.be/en/disinformation

> **European Centre of Excellence for Countering Hybrid Threats:**
https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

INFORMATION ON POTENTIAL FOREIGN INTERFERENCE:

> www.vsse.be (in FR and NL)

Everyone should follow the recommendations in this guide based on their own assessment of the risks. The recommendations were drawn up on the basis of the threat observed at the time of publication. We cannot guarantee that these recommendations will ensure the security of a targeted IT system.

SAFE SURFING DURING THE BELGIAN GENERAL ELECTION CAMPAIGN
Recommendations for a cybersecurity campaign

Safe surfing during the Belgian general election campaign
Recommendations for a cybersecurity campaign

Publisher: Francisca BOSTYN
King Albert II Avenue, 6 - 1000 Brussels

CENTRE FOR
CYBERSECURITY
BELGIUM

ADIV-SGRS

VSSE
veiligheid van de staat
sûreté de l'état

.be