

Security translated for Employees



Ine Segers
Ine.segers@devoteam.com



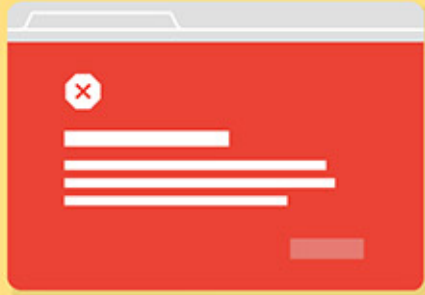
Topics

- Secure Surfing
- Recognize phishing
- If you get hacked
- Useful tools



Secure Surfing

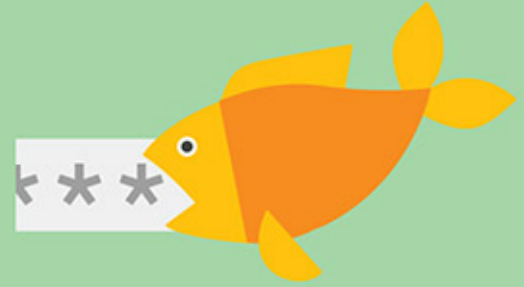
Safe Browsing



Malware

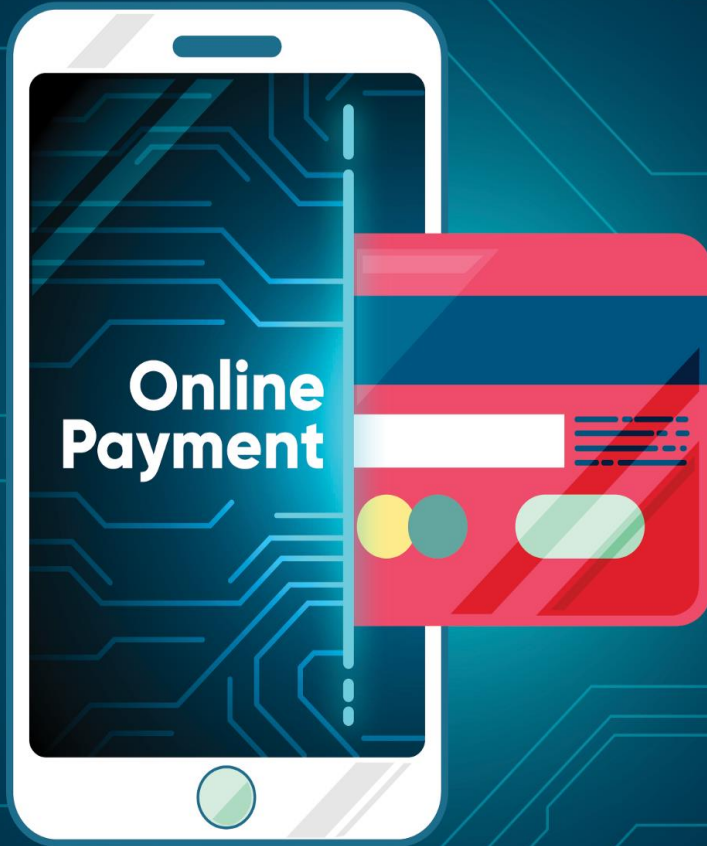


Unwanted Software



Social Engineering

[Use Safe Browsing in Chrome - Android - Google Chrome Help](#)
[Browse more safely with Microsoft Edge | Microsoft Learn](#)

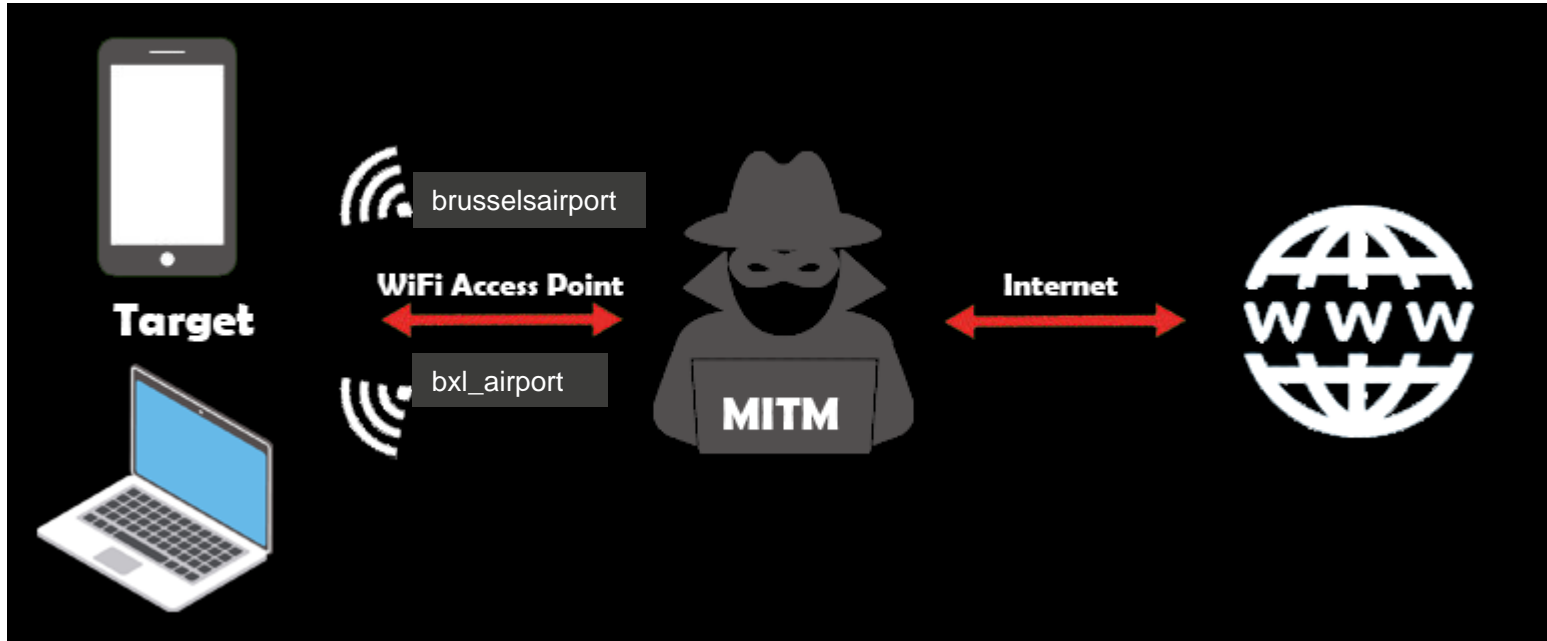


- You are asked to continue the sale outside of the website.
- You are asked to pay via a parcel or transport company.
- You are asked to perform a bank verification.
- The buyer offers you a higher amount than what you asked for.
- You are asked to pay a deposit to confirm the sale
- No padlock, no purchase: check if it uses "https://" rather than just "http://" in the URL



Be careful when connecting to free public wifi

In the train station, in stores, in airports... cybercriminals are using this same internet connection to monitor your activities. If possible, **use 4G/5G**



Don't tell ChatGPT your Secrets



What to avoid as input in ChatGPT



- Personal information
- Company sensitive information
- Company proprietary software

ChatGPT

Tips for getting started

■ Ask away

ChatGPT can answer questions, help you learn, write code, brainstorm together, and much more.

● Don't share sensitive info

Chat history may be reviewed or used to improve our services. Learn more about your choices in our [Help Center](#).

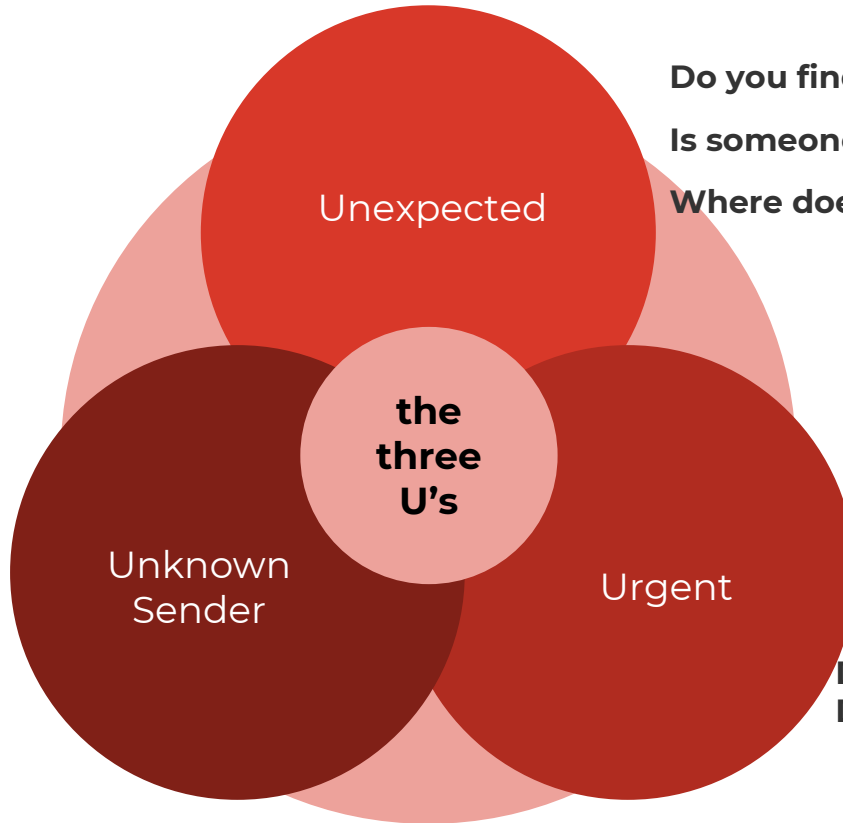
▲ Check your facts

While we have safeguards, ChatGPT may give you inaccurate information. It's not intended to give advice.

Okay, let's go

2

Recognizing Phishing Emails and Telephone Scams



Do you find the request strange?

Is someone trying to make you curious?

Where does the link you need to click on lead to?

**Did you really get a first reminder to pay?
Do you know that 'friend in need' ?**

Do you know the person who sent the e-mail?

From: Itsme Belgian Mobile ID <billing@pajilleros.net>
Sent: Monday 14 March 2022 18:54
To: [REDACTED]
Subject: Verleng uw toegang tot Itsme voor uw apparaat

OPGELET: Deze mail is afkomstig van een externe partij. Open geen bestanden en klik niet op links als u twijfelt aan de betrouwbaarheid van de correspondent. **Meld elke verdachte mail!**
ATTENTION : Ce courrier provient d'un tiers externe. N'ouvrez pas de fichiers et ne cliquez pas sur des liens si vous doutez de la fiabilité du correspondant.
Signalez tout courrier suspect !

Is dit bericht niet goed leesbaar? [Klik hier voor de onlineversie.](#)



Digitale veiligheid en privacy van het hoogste niveau

Je persoonsgegevens zijn belangrijk. Daarom volgt itsme® de Europese regelgeving voor elektronische identificatiemiddelen (eIDAS) en de Europese privacy-verordening (GDPR) waardoor je gegevens op de best mogelijke manier worden beschermd. Volgens de huidige wetgeving zijn gebruikers verplicht jaarlijks hun registratie opnieuw in te dienen om de gebruiksveiligheid van de app te waarborgen.

Check the Sender

Examples

Van: BE FEDERALE DGPF - CENTER <nanddebondt@gmail.com>



Federal employees don't use gmail

Datum: 14 december 2021 om 07:45:46 CET

Aan: CENTER BE DGPF <federal.info@politie.eu>



.eu is suspicious domain for Federal police

Onderwerp: RE: CSVNL.CONVOCATIE

ONDER UW AANDACHT

U WORDT BESCHULDIGD VAN EEN STRAFBAAR FEIT (ZIE DOSSIER)

Bijgesloten vindt u uw dagvaarding.

Na 72 uur, starten we een procedure, namelijk een arrestatiebevel.

Reageer alstublieft zo snel mogelijk.

(DGPF: Directoraat-generaal van de Federale Politie - **André DESENFANTS**)

Van: KBC Bank & Verzekering <no-reply@omi.uk>

Datum:

Aan:

Onderwerp: RE: Uw account is geblokkeerd

Antwoord aan: no-reply@omi.uk



.uk domain looks suspicious



Dubbele authenticatie !

Hallo,

Naar aanleiding van onze laatste verordening hebben wij een dubbele authenticatie ingesteld om onze gebruikers maximale veiligheid te garanderen.

Om de dubbele authenticatie te activeren, verzoeken wij u eerst zo snel mogelijk uw gegevens te bevestigen om er zeker van te zijn dat u de eigenaar van de rekening bent:

Identificeer jezelf

Look Closely for lookalike domains

Replacement:

Itsme.be

cocacola.com

Subdomains:

bnpparisbas.fortis.be

coca.colacom

Typo squatting:

financies.belgium.be

arnazon.com

Omission:

befius.be

micosoft.com




Check URL links


Van

Onderwerp: een document van de FOD Financiën is beschikbaar - Bericht van aanwending van een teruggave

Datum: 16 juni 2023

Aan:

 Vlaanderen

 **een document van de FOD Financiën is beschikbaar - Bericht van aanwending van een teruggave**
Overheidsdocumenten (eBox)

Beste

U hebt een nieuw eBox document van FOD Financiën ontvangen.
Bekijk uw eBox document op <https://asdkjwie1.info/> profiel.
Click or tap to follow link.

[Naar het document](#)

Right mouse click to verify URL

Smishing - SMS messages

Never click on the link, go directly to the bank or parcel service's web page or app




[Fluvius Belgium]
Gelieve uw persoonlijke terugbetaling te bevestigen via: min.lc/Fluvius-be

[Bpost]
Uw pakket is verzonden. Volg uw zending via:
<https://bpost-sorteercentrum.com/bpost/bezorging.php>

[Bpost]
Votre colis est au centre de tri. Appuyez sur le lien pour suivre votre colis:
<https://bpost-sorteercentrum.com/bpost/bezorging.php>

3

And if you get
hacked



YOU HAVE BEEN HACKED

1. **Change password:** If you have entered a password that you also use elsewhere, change it immediately. Change it everywhere you use it.
2. **Notify Card stop** : If you have entered your credit card or debit card details, notify [Card Stop](#) 078 170 170 (+32 78 170 170 from abroad).
3. **Contact your bank immediately,** to block your last payment and possibly also your account.
4. **Contact the police:** If you notice that money has been stolen from your bank account, be sure to file a complaint with the police.
5. **Inform Safe on web:** Forward the suspicious message you clicked on to suspicious@safeonweb.be
6. **Avoid to pay Ransom:** you have no guarantee whatsoever that you will recover your data in a safely. Check www.nomoreransom.org to see whether the key for this ransomware is available. Perform a full reinstallation of your device and [use a backup to restore your data.](#)

<http://www.safeonweb.be>



Help! I clicked on a fake link

Identifying phishing websites in time



My data has been stolen

Check it now!



Help! My camera footage is online!

Internet of Things



Help! My device has been taken over

My device has been taken over by a virus that is asking for a ransom!



Help, I have a virus!



I am getting a lot of spam and phishing e-mails in my inbox

Avoid your e-mail address ending up on a list used by spammers or phishers



Ok is not always OK !

Discover the new campaign



First aid

Do you have a problem?



How safe are you?

Do our tests



Safe on internet

Tips

⚠ News

- 14 Sep 2023: Expecting a parcel? Watch out for suspicious ...
- 07 Sep 2023: Beware: the "sextortion" scam is back!
- 25 Aug 2023: Protect yourself from phone scams (often ...
- 18 Aug 2023: Beware techscams (Microsoft scams) ...
- 11 Aug 2023: New phone scam targeting Itsme users
- 02 Aug 2023: Your life is in danger! Hitman scam ...
- 24 Jul 2023: Beware of false warning about unpaid ...
- 20 Jul 2023: More reports of phishing and smishing ...
- 19 Jul 2023: Dozens of reports of CEO fraud
- 17 Jul 2023: Fake text message appearing to be from ...

[Read more >](#)

4+

Useful tools

Install the Safeonweb App



Are your passwords circulating on the Internet ?

You can check for yourself on the [Haveibeenpwned](#) website.

';--have i been pwned?

Check if your email address is in a data breach

email address

pwned?



Interactive Cyber Security E-Learning via Kahoot

Challenge your employees with an interactive e-learning via Kahoot and raise awareness on cyber security topics.

RELEASED NOVEMBER 2022



SME Security Scan

Are your computer infrastructure and files well protected? Do the test.

RELEASED NOVEMBER 2022



Cyber Security KIT

The Cyber Security KIT: for SMEs and organizations raise awareness about cyber security among their employees.

RELEASED NOVEMBER 2022



Start with Cybersecurity: the basics

The "Start with Cybersecurity: the basics" guide helps startups and online business enhance their strategy around cybersecurity.

[EDUbox Cybersecurity \(NL\)](#)

[EDUbox Cybersecurité \(FR\)](#)



Cybersecurity: Digitale bescherming als goede gewoonte

DIGITALE COMPETENTIE | BURGERSCHAP | KENNIS- EN SYSTEMENKENNEN | SOCIAAL-RELATIONELE COMPETENTIE

In de EDUbox 'Cybersecurity: digitale bescherming als goede gewoonte' komen jongeren te weten hoe ze zich tegen cybercriminelen kunnen beschermen. Broodnodig, want overal liggen hackers op de loer om hun gegevens of eigendommen te stelen. Welke trucs passen ze toe? En hoe kunnen jongeren hun eigen digitale veiligheid verhogen? In deze EDUbox leren ze alles over hun digitale voetafdruk.

meer info

bestel de eduboxen | lees de handleiding

DEZE EDUBOX IS OOK BESCHIKBAAR IN ANDERE FORMATS:

in groep | individueel

download de pdf | open de interactieve site | bekijk de interactieve video

Ook beschikbaar in andere talen:

Download en print zelf de integrale EDUbox | Doorloop de EDUbox online met geïntegreerde video's en weblinks. | In de videoles treedt de leerling in interactie met een VRT-journalist. Deze kan individueel gevolgd worden.

