16 Oct 2023 -15:51

Phishing, the devil's in the details! Install the Safeonweb browser extension and never get caught out again

Campaign provides internet users with new online safety tools

On 16 November, the Centre for Cybersecurity Belgium (CCB), Febelfin and the Cyber Security Coalition will launch a striking awareness campaign about phishing: *Phishing: The devil's in the details!* This type of online scam is on the rise and continues to claim countless victims, both private individuals and companies and organisations.

Phishing in numbers

- A total of 39.8 million EUR was stolen as a result of phishing in 2022, which is more than last year (2021: 25 million EUR). This is mainly due to the huge increase in the number of phishing messages sent.
- 69% of Belgians have received at least one phishing message in the past 6 months (source: Febelfin together with IndiVille, March 2023)
- 8% of Belgians have never heard of phishing. The older age group scores better in this respect, as 4% have never heard of phishing, which is an improvement from 2022 (7%). Although there is a slight improvement from 2021 (24%) and 2022 (30%), the number of young people who are unfamiliar with phishing is still too high (23%).

- 8% of Belgians say they have been victims of phishing. Among young people, this percentage is higher at 12%.
- Only 62% of Belgians who fell victim to phishing knew what steps to take.

Source: storytelling_phishing_nl_230602.pdf (febelfin.be)

- From January to September 2023, more than 7 million messages have already been sent to suspect@safeonweb.be, surpassing the record figure for 2022, when we received about 6 million messages.
- This represents an average of 26,425 messages per day.
- In a recent survey commissioned by the Centre for Cybersecurity Belgium (September 2023), 28% of respondents said they did not know how to recognise a fake website.
- 78% said they would never click on a suspect link, although 22% might.
- 57% of respondents believe that there is a high probability that they will one day fall victim to phishing.
- Over 600 partners join the Safeonweb (CCB) campaign every year. In recent years, this has enabled us to reach half of the Belgian population (+18 years old).

Source: Safeonweb, 2023

"Phishing messages are a real curse. They are circulating on a massive scale all the time, and are constantly claiming victims.Why can't we get rid of this phenomenon? It's fairly easy to arouse curiosity or fear in human beings. We can't resist a tempting offer. Phishers capitalise on these typically human characteristics.They try to approach and convince their victims using a whole range of tricks.This is precisely the meaning of the term "social engineering".

What's more, phishing messages are increasingly difficult to unmask: they are professionally formatted, link to very convincing websites, etc., and crooks have also understood the opportunity to use various AI applications to send convincing, attractive and personalised messages."

Miguel De Bruycker
Director General of the Centre for Cybersecurity Belgium

Why can't we just get rid of phishing?

Phishing is not a new phenomenon. Phishing has always been around. Fraudsters try to get their hands on your (bank) details through various channels such as e-mail, phone, letter, text message, social media or WhatsApp. They try to scam people by posing as trustworthy organisations or institutions (banks, government departments, utility companies, etc.).

They send messages containing links to fake websites, where victims are asked to enter personal bank codes. Once the fraudsters get their hands on these personal bank codes, they can carry out transactions

on behalf of the victim.

Phishing is a real scourge. Large numbers of messages continue to circulate and trip up victims. Why can't we just get rid of phishing? There are several reasons for this. It's in our human nature to be curious or get frightened. We simply cannot resist an attractive offer. Phishers capitalise on this. They try to approach and convince their victims through all kinds of excuses. This is called social engineering.

Phishing messages are also increasingly difficult to detect: they rarely contain spelling mistakes anymore, are professionally formatted, refer to very convincing looking websites, etc. The cybercriminals have become real professionals. The future does not really look very bright. AI opens up many new positive prospects, but scammers will also be only too happy to use various applications to send persuasive, attractive and personalised messages.

Phishing: The devil’s in the details!

However, it is not impossible to identify phishing messages and phishing websites. The devil’s in the details. To make sure you never click on a link leading to scam website, you should learn to read the website's URL. How?
Hover your mouse over the link. If the domain name, i.e., the word before .be, .com, .eu, .org, etc. and before the very first slash "/" really is the name of the organisation you are looking for, then you can trust the website. But if you see something else there, an odd combination, or the domain you expect but with a slight difference, be careful!

For example:

- The domain is safeonweb for the link www.safeonweb.be/tips. In this example, you will be taken to the correct website.
- If the link is www.safeonweb.tips.be/safeonweb, "tips" is the domain, and you will be taken to another website.

Scammers will use URLs that are slightly different. So always look very carefully at the URL before clicking on it. When in doubt, don't click on a link in a post, but go to the website yourself by typing the URL you know and generally use into your browser bar.

Centre for Cyber Security Belgium launches Safeonweb browser extension

As it is still very difficult for many people to properly read and understand a URL, we are launching a new tool: the Safeonweb Browser extension, which will help you determine the reliability of any website you visit. The extension assigns a trust level to each website: high, medium or low. This trust level is based on known factors about the website's domain, its owner and the certification level obtained from a certification authority.

The call to action to the campaign is therefore: Install the Safeonweb extension for your browser. It will alert you when you visit a website that's unsafe and when it is dangerous to enter your details.

In addition to the Safeonweb browser extension, Safeonweb has 3 other tools:

- E-mail address: suspicious@safeonweb.be
- Safeonweb application: https://safeonweb.be/en/safeonweb-app
- Safeonweb e-learning: https://surfwithoutworries.safeonweb.be/en/modules

Febelfin challenges you with the Hacker Hotline

With the *Hacker Hotline*, a mobile escape game, Febelfin wants to make young people aware of the dangers of online fraud in a fun way. It should also help them to arm themselves against these practices. Players are challenged to outsmart the cybercriminal/phisher... This game is an ideal complement to this new national awareness campaign, because you can only win the game if you pay attention to the details.

About the game itself

Anyone can fall victim to online fraud. On the Hacker Hotline, you are the point of contact for victims of phishing and scams. Your task is to provide help - via a telephone and video hotline - to people under stress, in a race against time. The game gets even more exciting when the hacker suddenly appears in the scenario.

The *Hacker Hotline* is a collaboration between Febelfin and the creative agency Hurae.

> "The "Hacker Hotline" is a mobile escape game in which Febelfin targets young people, partners, schools and events to raise awareness of forms of online fraud such as phishing. The game allows you to explore the techniques used by fraudsters to trap their victims and learn how to arm yourself against this type of fraud. If you manage to escape the bus, you'll have all the tools you need to navigate safely online in real life. At the same time, you will learn fundamental concepts such as two-factor authentication and what is meant by a strong password."

Karel Baert
CEO Febelfin.

Campaigning together

Only by cooperating with governments, the police, the judiciary, the telecom sector, etc., can we tackle phishing. That is why the CCB, Febelfin and the Cyber Security Coalition, together with more than 600 partners, have joined forces for a new, broad-based awareness campaign that aims to inform and warn people. After all, Internet users have to become more vigilant. Alert members of the public are extra cautious, and that is the purpose of this awareness-raising campaign.

The aim is to appeal to the widest possible audience to make sure the campaign is heard by everyone. The campaign will run on various channels: the key message will be delivered via TV ads and in cinemas. Social media will also be used to raise awareness of the dangers of phishing. All campaign material can be downloaded at https://safeonweb.be/en/campaign-material

"Every year, the threat landscape continues to evolve, demanding a collective response from industry, government, academia and citizens.The national awareness campaign run by the CCB and its partners provides an essential platform for all stakeholders to play an active role in strengthening our digital defences."

Séverine Waterbley
President of FPS Economy and Cyber Security Coalition Board Member

More information

Please contact the Centre for Cybersecurity Belgium or Febelfin for more information:

Centre for Cybersecurity Belgium:
Katrien Eggers via katrien.eggers@ccb.belgium.be, 0485765336
Michele Rignanese via michele.rignanese@ccb.belgium.be, 0477 38 87 50
Febelfin: Isabelle Marchand via press@febelfin.be or 02/507.68.31

Who is who?

About the Centre for Cybersecurity Belgium

The Centre for Cybersecurity Belgium (CCB) is the national reference body for cybersecurity in Belgium. The CCB supervises, coordinates and monitors the implementation of the Belgian cybersecurity strategy. Optimum information sharing enables businesses, public authorities, essential service providers and the general public to protect themselves adequately. For more information, visit www.ccb.belgium.be

About Febelfin

Febelfin is the representative federation of the Belgian banking sector. As an industry federation, we provide a voice for banks and represent our members to policy makers, regulators, industry federations and interest groups. Febelfin represents around 245 financial institutions in Belgium. Febelfin's mission is to develop a financial sector that serves society.

About the Cyber Security Coalition

The mission of the Cyber Security Coalition is to strengthen Belgium's cybersecurity resilience by developing a robust national cybersecurity ecosystem. This can be achieved by bringing together the skills and expertise of academia, business and government in a trusted platform. This platform focuses on promoting information sharing, operational cooperation, developing recommendations for more effective policies and guidelines, and implementing joint awareness-raising campaigns for citizens and organisations. More than 1,200 representatives from our 160 member organisations participate in our activities and contribute to our mission.

Centre for Cyber Security Belgium
Rue de la Loi 18
1000 Brussels
Belgium
http://www.ccb.belgium.be

Katrien Eggers
Spokesperson(NL/FR/E)
+32 485 76 53 36
katrien.eggers@ccb.belgium.be

Michele Rignanese
Spokesperson(NL/FR/E)
+32 (0)477 38 87 50
michele.rignanese@ccb.belgium.be