29 Jan 2025 -08:39

44% of Belgians forward phishing messages to suspicious@safeonweb.be

In 2024, observant citizens forwarded more than 9 million messages to suspicious@safeonweb.be . In record year 2023, there were 10 million. On average in 2024, we received 25,900 messages per day. We would like to sincerely thank all internet users who continue to do so! Together we are making the internet a safer place.

With this information, we were able to detect and redirect exactly 1,644,732 suspicious links. Indeed, less attentive internet users who do click on such a link are redirected by us to a warning page and thus not scammed.

A survey by the Centre for Cybersecurity Belgium (Safeonweb, 12/2024) shows that 44% of Belgians forward messages to suspicious@safeonweb.be . In 2023 the figure was 39%, so the email address remains attractive. For us, this is a special source of information that we use primarily for our phishing shield (BAPS System), but also to warn citizens.

Thanks to all these messages, we can publish targeted alerts on Safeonweb.be, Facebook, Instagram and X about phishing messages circulating. We also send these 'alerts' via the Safeonweb App. In 2024, we published 81 alerts on the most common current phishing messages.

Phishing? Nothing new under the sun. Or is there?

Phishing will remain one of the most used and evolving attack methods in cybercrime in 2024. (See ENISA Threat Landscape, 2024)

At first glance, most phishing messages are very similar to those of recent years. You have the messages that seem to come from government departments, police, banks, Itsme, etc., as well as offers in the 'too good to be true' category, from unlikely promotions, to one-off bargains, and even the 'lost inheritance' resurfaced

Scammers still follow current events very closely and use current events to give credibility to their phishing messages. For example, year after year around the end-of-year period, we see more messages appearing around Christmas promotions or packages to be delivered.

Still, we see 5 shifts

1. Smishing and vishing are on the rise

Smishing (phishing via SMS) and vishing (phishing via phone calls) are on the rise. Cybercriminals use this to directly extract response and 2FA codes. An example. They call their victim and pretend to be someone from Cardstop who wants to help because a suspicious transaction allegedly happened on the bank account. The scammer will convince the victim to e.g. pass on response codes or open Itsme and complete authentication.

2. More phishing via social media

Platforms such as LinkedIn, Facebook, Instagram and WhatsApp are increasingly used to spread phishing links. The principles are the same as for phishing by email or text message.

3. More personalised attacks

Leaked personal data from previous data breaches personalise attacks, increasing the credibility of phishing, as well as smishing and vishing. Scammers use this data to gain your trust. If you receive a call from a so-called bank employee who knows your name, date of birth and other details, you are inclined to believe that this is really a bank employee.

4. AI and deepfake technology make phishing more credible

Cybercriminals are undoubtedly using AI more frequently to personalise phishing messages, making them more convincing. Deepfake audio and video can be deployed to refine CEO fraud and spearphishing, by mimicking the voice of a company's CEO. While such practices are certainly possible at the moment, we have yet to detect any concrete examples.

5. Https is no guarantee of security

Year after year, we notice that more criminals are using SSL certificates to make their phishing URLs look more trustworthy. Specifically, this means that, as an internet user, you can no longer assume that a URL starting with https is by definition secure.

Belgisch Anti-Phishing Shield (BAPS)

This phishing shield protects the citizens of our country from cyber criminals. It is the showpiece of the Centre for Cybersecurity Belgium (CCB). This cutting-edge technology puts us, as a small country, among the absolute world leaders.

How does it work?

1. The Centre for Cybersecurity Belgium (CCB) receives information about potentially malicious websites when internet users forward suspicious messages to suspicious@safeonweb.be.

2. Attachments and other links are then extracted from the suspicious messages. The URLs are also extracted from screenshots and QR codes.

3. It analyses the URL/link/attachment. If it turns out to be a malicious site, it is listed and sent to our partners (ISPs, Google Safe Browsing and Microsoft SmartScreen).

4. When an internet user clicks on a link leading to a malicious site, the ISP in question compares the DNS request with the list of malicious sites.
5. The user is then redirected to a warning page and cannot visit the malicious site.

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