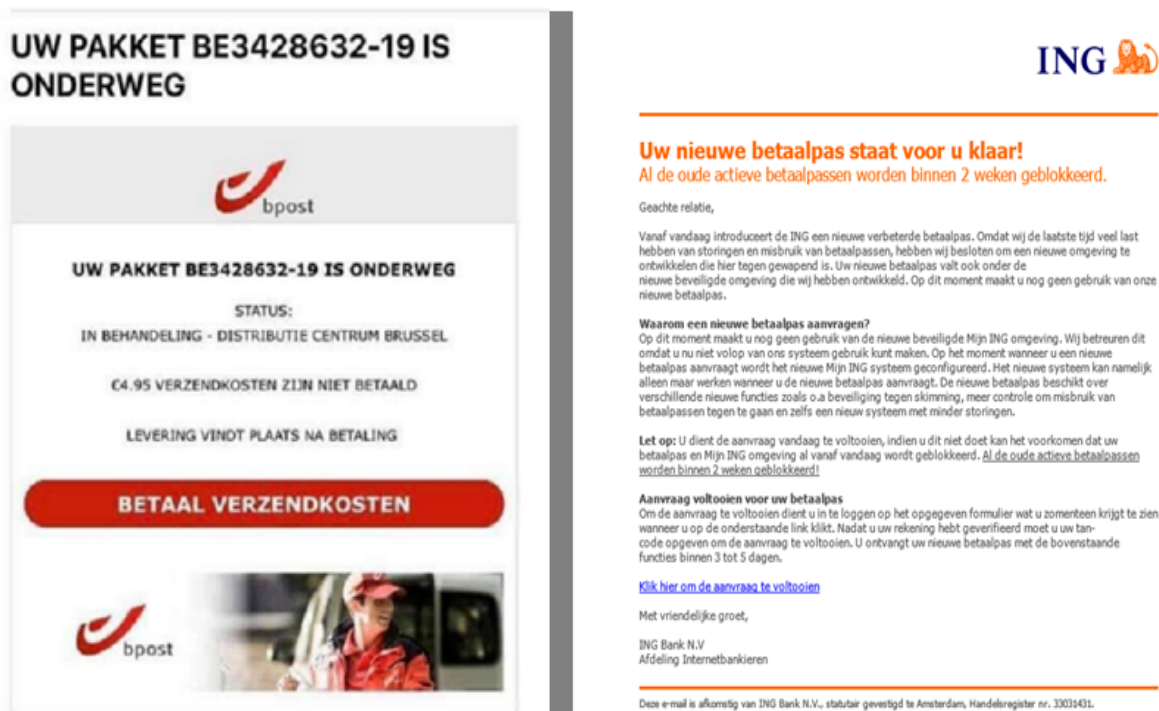


Phishing: the new burglary in 2021?

34,000,000 euros.¹ That is the total amount that phishers were able to steal in the year 2020. What is phishing and how do these cybercriminals operate? Will I get my money back if I am scammed and how do I recognize fake e-mails? An overview.

Phishing?

Phishing is a form of cybercrime in which the potential victim is approached via e-mail, text message, social media or telephone. The scammer pretends to be someone else in an attempt to gain access to the confidential data of victims. It is similar to Internet fraud except that the perpetrator does not manipulate data, but people. It is a form of psychology to gain the victim's trust. Phishers work very ingeniously and skillfully respond to current events. Messages from a bank, a technology company or a postal service that says a parcel is waiting for you, the chance that you have received one of these messages is very high.



UW PAKKET BE3428632-19 IS ONDERWEG

ING

Uw nieuwe betaalpas staat voor u klaar!
Al de oude actieve betaalpassen worden binnen 2 weken geblokkeerd.

Geachte relatie,

Vanaf vandaag introduceert de ING een nieuwe verbeterde betaalpas. Omdat wij de laatste tijd veel last hebben van storingen en misbruik van betaalpassen, hebben wij besloten om een nieuwe omgeving te ontwikkelen die hier tegen gewapend is. Uw nieuwe betaalpas valt ook onder de nieuwe beveiligde omgeving die wij hebben ontwikkeld. Op dit moment maakt u nog geen gebruik van onze nieuwe betaalpas.

Waarom een nieuwe betaalpas aanvragen?
Op dit moment maakt u nog geen gebruik van de nieuwe beveiligde Mijn ING omgeving. Wij betreuren dit omdat u nu niet volop van ons systeem gebruik kunt maken. Op het moment wanneer u een nieuwe betaalpas aanvraagt wordt het nieuwe Mijn ING systeem geconfigureerd. Het nieuwe systeem kan namelijk alleen maar werken wanneer u de nieuwe betaalpas aanvraagt. De nieuwe betaalpas beschikt over verschillende nieuwe functies zoals o.a. beveiliging tegen skimming, meer controle om misbruik van betaalpassen tegen te gaan en zelfs een nieuw systeem met minder storingen.

Let op: U dient de aanvraag vandaag te voltooien, indien u dit niet doet kan het voorkomen dat uw betaalpas en Mijn ING omgeving al vanaf vandaag wordt geblokkeerd. Al de oude actieve betaalpassen worden binnen 2 weken geblokkeerd!

Aanvraag voltooien voor uw betaalpas
Om de aanvraag te voltooien dient u in te loggen op het opgegeven formulier wat u zometeen krijgt te zien wanneer u op de onderstaande link klikt. Nadat u uw rekening hebt geverifieerd moet u uw tan-code opgeven om de aanvraag te voltooien. U ontvangt uw nieuwe betaalpas met de bovenstaande functies binnen 3 tot 5 dagen.

[Klik hier om de aanvraag te voltooien](#)

Met vriendelijke groet,

ING Bank N.V.
Afdeling Internetbankieren

Deze e-mail is afkomstig van ING Bank N.V., statutair gevestigd te Amsterdam, Handelsregister nr. 33031431.

¹ <https://www.febelfin.be/nl/press-room/phishing-2020-de-cijfers>



Federale
Overheidsdienst
FINANCIEN

Geachte heer/mevrouw,

Op 16 oktober heeft de overheid besloten om elk huishouden een bedrag van €202,68 toe te kennen ter compensatie van uw energie en waterfactuur.

Ter identificatie en controle is het van belang om een verificatie na te gaan om dit proces te vervolledigen. Vervolgens zal u het bedrag binnen enkele werkdagen ontvangen.

Wat heeft u hiervoor nodig?

- Bankkaart
- Kaartlezer

Via de onderstaande link kunt u het verificatie proces terugvinden.

Covid-19 compensatie

Let op: Indien u de verificatie niet juist heeft volbracht, hebt u geen recht op een compensatie.

Wij vertrouwen erop u voldoende te hebben geïnformeerd.

Met vriendelijke groeten,
Federale Overheidsdienst Financiën

Disclaimer Privacy Policy

Dit is een automatisch verstuurd bericht. Het is niet mogelijk om te antwoorden op dit bericht.

The phenomenon of phishing, or "fishing" for sensitive data such as passwords and bank or credit card details, has grown exponentially in recent years. In 2020, no fewer than 3,200,000 suspicious messages were forwarded to the Centre for Cybersecurity Belgium (CCB). In the first half of last year, the police services drew up 3,438 official reports on phishing. A fourfold increase compared to the previous year. But that is only the tip of the iceberg, according to the Public Prosecutor's Office.²

There are various reasons for this growth. Firstly, the number of phishing messages is increasing exponentially, so that the Public Prosecutor's Office simply cannot process the flood of files anymore. It seems almost like an unpleasant side effect of the corona crisis, now that contacts are more and more made digitally. Considering the many victims and the limited human and material resources of the judiciary, the chance that offenders will be caught is rather small.



² <https://www.vrt.be/vrtnu/a-z/pano/2021/pano-s2021a7/>.

In addition, the anonymity of the perpetrator is an important explanatory factor. Safely from behind his computer screen, a cybercriminal can rob thousands of people at the same time under the radar of the justice department, since in many cases they are unable to find out the identity of the person who sends fake messages or sets up a fake website. Perpetrators imagine they have impunity.

Finally, phishing is a piece of cake. You do not need to be a computer wizard to do phishing. It is just a matter of gaining the trust of victims in order to steal sensitive information and money.

How do these cybercriminals operate?

Quite simply. Phishing often has a structured organization. At the top of the pyramid are the IT experts who create software programs in which they can create credible phishing sites and e-mails. By hacking into websites where people have registered, the fraudsters obtain data that is sold in closed chat groups via online marketplaces. Phishers buy the data from the software programs and choose their victims from this list. In this way phishers can often mail thousands of people at the same time. At the bottom are the money mules. The victims' money that the phishers steal ends up in their accounts. In other words, a kind of diversionary tactic for the judicial authorities, because this way not only do the gang leaders often remain out of the picture for the investigators, but the phishers are also barely traceable.

Will I get my money back?

Perhaps the most important question for victims is: will I get my money back? It is essential that victims act quickly. If you feel that a transaction is suspicious, contact your bank immediately. They have access to your accounts and the authority to block them. The chance of you being on time does seem smaller now that the money has definitely left the bank from the moment the order was given. This is why banks are working together to have accounts blocked as soon as possible. As soon as a bank is informed of a phishing case, the victim's bank will contact the bank of the money mule. In other words, the bank to which the money is transferred. They will try to block the funds and recover them afterwards.

If this does not work and the money has already disappeared, there is a possibility of compensation from your bank. The bank will make a balance of interests as to whether you, as a client, can be held liable or not. For this, the bank uses the figure of 'gross negligence'³. In each situation, they will look at which fraud technique was used and whether customers were too careless in sharing their personal data - albeit under pressure and in good faith - with a cybercriminal. In any case, the burden of proof is on the bank and it is not up to you to prove that you were not negligent.

The figure of 'gross negligence' is subject in many heated debates, as the law does not clearly define what can be understood as 'gross negligence'.

³ https://www.standaard.be/cnt/dmf20210507_97478909

Testaankoop⁴ believes that banks invoke this concept all the time to avoid paying back the money or to pay less. Examples of 'gross negligence' include not blocking your bank card or not keeping the card together with the code or not entrusting it to anyone. But it is very difficult to make a general statement. In practice, many banks do refund the customer in many cases.⁵

If the bank decides that you are responsible and you think it's unfair, do not hesitate to raise your conflict with Ombudsfin⁶, the mediation service for financial disputes. This is an independent institution that can mediate in disputes about fraudulent transactions and refunds between the victim and the bank.

How do I recognize false messages?

Phishers are very inventive and regularly invent new tricks to get people out of money or data. In addition, the scamming methods are also becoming increasingly difficult to recognize. It seems almost impossible to distinguish false e-mails and reliable messages. Below, we have listed a number of tips for assessing whether you can trust a message.

Do you doubt that a message is suspicious? Then briefly answer these questions for yourself:⁷

- | | | |
|---|---|---|
| 1. Is it unexpected? | 2. Is it urgent? | 3. Do you know the sender? |
| 4. Do you find the question strange? | 5. Where does the link you have to click on lead to?
Tip: move over the link and see where it takes you. It is best not to open a suspicious link. | 6. Are you addressed personally? |
| 7. Does the message contain many language errors? | 8. Is the message in your Spam? | 9. Is someone trying to make you curious? |

Are you uncomfortable about a certain transaction you made? Contact Card Stop as soon as possible to have your card blocked. You can do this by calling 070 344 344. Please note that Card Stop will never call people. If someone

⁴ <https://www.test-aankoop.be/geld/betalen/dossier/betaalkaarten-hoe-krijgt-u-uw-geld-terug/dief-heeft-uw-kaart-of-gegevens>.

⁵ <https://www.vrt.be/vrtnu/a-z/pano/2021/pano-s2021a7/>

⁶ <https://www.ombudsfin.be/>

⁷ <https://www.safeonweb.be/nl/leer-valse-mails-herkennen>

pretends to be a Card Stop employee on the phone, this person is 100% a fraudster.

It is also important to gather as much evidence as possible. Always make a note of all the details you received from the scammers, such as phone numbers and names. If necessary, take screenshots of the forged e-mails, links and website. With this evidence in your pocket, you can easily file a report with the police and have an official report drawn up.

Finally, never give personal codes such as your PIN number or response code. The bank will never ask for these codes through any channel whatsoever. In general, don't be too naive. A message that is too good to be true, usually is. In addition, phishers often play on the feeling that things have to happen fast. So be alert for messages that have a certain urgency behind them. Do not blindly believe every e-mail or text message, but also do not believe that it will never happen to you. Be on your guard and double check!

If you come across a suspicious message while surfing the Internet, do not hesitate to forward it to verdacht@safeonweb.be. They check the links and attachments of these forwarded messages and are able to block suspicious links. In this way, less attentive Internet users who have clicked on the link are also protected. By acting quickly, cyber criminals are less likely to make victims. Better safe than sorry.

If you still have questions about phishing after reading this article, do not hesitate to contact us via joost.peeters@studio-legale.be, simon.geens@studio-legale.be or 03 216 70 70.