Phishing: het nieuwe inbreken anno 2021?

written by Dennis_ Rombaut_ | oktober 25, 2021

Phishing: het nieuwe inbreken anno 2021?

34.000.000 euro.[1] Dat is het totale bedrag dat phishers in het jaar 2020 konden stelen. Wat is phishing en hoe gaan deze cybercriminelen te werk? Krijg ik mijn geld terug als ik word opgelicht en hoe herken ik valse e-mails? Wij zochten het voor u uit.

Phishing?

Phishing is een vorm van cybercriminaliteit waarbij het potentiële slachtoffer wordt benaderd via e-mail, sms, sociale media of telefoon. De oplichter doet zich daarbij voor als iemand anders in een poging toegang te krijgen tot de vertrouwelijke gegevens van slachtoffers. Het lijkt op internetfraude, met dit verschil dat de dader geen gegevens manipuleert, maar wel personen. Het is een vorm van psychologie om op die manier het vertrouwen te winnen van het slachtoffer. Phishers gaan hierbij zeer ingenieus te werk en spelen handig in op de actualiteit. Berichtjes van een bank, een technologiebedrijf of een postbedrijf dat zegt dat er een pakje op je wacht, de kans dat u één van deze berichtjes heeft ontvangen, is bijzonder groot.

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

Het fenomeen van phishing of “hengelen” naar gevoelige gegevens zoals wachtwoorden en bank- of kredietkaartgegevens is de laatste jaren exponentieel gegroeid. In 2020 werden er maar liefst 3.200.000 verdachte berichten doorgestuurd naar het Centrum voor Cybersecurity België (CCB). In de eerste helft van vorig jaar stelde de politiediensten 3.438 pv’s rond phishing op. Een viervoudiging in vergelijking met het jaar ervoor. Maar dat is nog maar het topje van de ijsberg, weet het Parket.[2]

Verschillende redenen liggen hiervoor aan de basis. Ten eerste stijgt het aantal phisingberichten exponentieel waardoor Justitie de toevloed aan dossiers simpelweg niet meer kan verwerken. Het lijkt haast een onaangename bijwerking

van de coronacrisis, nu contacten steeds vaker digitaal verlopen. Gezien de vele slachtoffers en beperkte mensen en middelen bij Justitie is de kans dat daders gepakt worden eerder klein.

Daarnaast is de anonimiteit waarin de dader vertoeft een belangrijke verklarende factor. Veilig van achter zijn computerscherm kan een cybercrimineel onder de radar van Justitie duizenden mensen tegelijk bestelen, nu zij in veel gevallen niet in staat zijn de identiteit te achterhalen van de persoon die valse berichten stuurt of een valse website opzet. Daders wanen zich straffeloos.

Tot slot, phishing is kinderspel. Je hoeft helemaal geen computerwizard te zijn om aan phishing te kunnen doen. Het is een kwestie van het vertrouwen te winnen van slachtoffers om op die manier gevoelige informatie te ontfutselen en vervolgens geld te stelen.

Hoe gaan deze cybercriminelen te werk?

Heel eenvoudig. Phishing kent vaak een gestructureerde organisatie. Bovenaan de piramide staan de IT-experten die softwareprogramma's maken waarmee zij geloofwaardige phishingsites en -mails kunnen maken. Door websites te hacken waarop personen zich hebben aangemeld, komen de oplichters aan data die via online marktplaatsen aangeboden worden in gesloten chatgroepen. Phishers kopen de data die voortkomen uit de softwareprogramma's en kiezen uit deze lijst hun slachtoffers. Op die manier kunnen phishers vaak duizenden mensen tegelijkertijd mailen. Onderaan staan de geldezels. Op hun rekeningen komt het geld van de slachtoffers terecht dat de phishers stelen. Met andere woorden een soort van afleidingsmanoeuvre voor Justitie, want zo blijven niet enkel de bendeleiders vaak buiten beeld bij de speurders, maar zijn ook de phishers amper te traceren.

Krijg ik mijn geld terug?

Misschien wel de belangrijkste vraag voor slachtoffers: krijg ik mijn geld terug? Essentieel hierbij is dat slachtoffers snel handelen. Heb je het gevoel dat een transactie bij nader inzien toch verdacht is, contacteer dan onmiddellijk uw bank. Zij kunnen de toegang tot jouw rekeningen laten blokkeren. De kans dat je op tijd bent, lijkt wel kleiner nu het geld definitief vertrekt vanaf het moment dat daartoe de opdracht werd gegeven. Vandaar dat banken samenwerken om zo snel mogelijk rekeningen te laten blokkeren. Zodra een bank op de hoogte wordt gesteld van een phishinggeval, zal de bank van het slachtoffer contact opnemen met de bank van de geldezel. Met andere woorden de bank naar waar het geld getransfereerd wordt. Zij proberen alsnog de gelden te blokkeren en achteraf te

gaan recupereren.

Lukt dit niet en is er reeds geld verdwenen, dan staat er een mogelijkheid open tot schadevergoeding van uw bank. Deze laatste zal een belangenafweging maken omtrent de vraag of je als klant aansprakelijk kan gesteld worden of niet. Hiervoor gebruikt de bank de figuur van de 'grove nalatigheid'.[3] Men zal per situatie gaan kijken naar welke fraudetechniek gehanteerd werd en of klanten té onvoorzichtig geweest zijn door hun persoonsgegevens – weliswaar onder druk en te goeder trouw – te delen met een cybercrimineel. In elk geval is het zo dat de bewijslast rust bij de bank en het dus niet aan u is om te bewijzen dat je niet nalatig bent geweest.

Over de figuur van de 'grove nalatigheid' woeden de hevigste discussies, nu de wet niet duidelijk omschrijft wat wel en wat niet onder 'grove nalatigheid' dient te worden verstaan. Testaankoop[4] vindt dan ook dat banken te pas en te onpas dit begrip inroepen om niet of minder te moeten terugbetalen. Voorbeelden van 'grove nalatigheid' zijn onder andere het nalaten van je bankkaart te laten blokkeren of de kaart samen met de code te bewaren of aan iemand toe te vertrouwen. Maar het is heel moeilijk om daar een algemene lijn in te trekken. In de praktijk is het immers wel zo dat heel wat banken, in heel wat gevallen, de klant terugbetalen.[5]

Schuift de bank de volledige aansprakelijkheid in uw schoenen en denk je als slachtoffer in uw recht te staan, aarzel dan niet om je conflict aan te kaarten bij Ombudsfin[6], de ombudsdienst voor financiële geschillen. Dat is een onafhankelijke instelling die kan bemiddelen omtrent betwistingen over frauduleuze verrichtingen en terugbetalingen tussen slachtoffer en bank.

Hoe herken ik valse berichten?

Phishers blijken zeer vindingrijk en bedenken geregeld nieuwe kunstgrepen om mensen geld of gegevens afhandig te maken. Daarnaast zijn de oplichtingsmethodes ook steeds moeilijker te herkennen. Het onderscheid maken tussen valse e-mails en betrouwbare berichten, het lijkt haast een onmogelijke opdracht. Hieronder zetten we een aantal tips op een rijtje om te beoordelen of je een bericht kan vertrouwen.

Twijfel je of een bericht verdacht is? Beantwoord dan kort voor jezelf deze vragen:[7]

1. Is het onverwacht?
2. Is het dringend?
3. Ken je de afzender?

4. Vind je de vraag vreemd?
5. Naar waar leidt de link waar je moet op klikken? Tip: beweeg over de link en kijk waar deze u naartoe stuurt. Een verdachte link doet u best niet open.
6. Word je persoonlijk aangesproken?
7. Bevat het bericht veel taalfouten?
8. Zit het bericht in je Spam?
9. Probeert iemand je nieuwsgierig te maken?

Zit er een reukje aan een bepaalde transactie die je hebt verricht? Contacteer zo snel mogelijk Card Stop om je kaart te laten blokkeren. Dit kan op het nummer 070 344 344. Weet dat Card Stop nooit mensen zal opbellen. Geeft iemand zich aan de telefoon uit als een medewerker van Card Stop, dan is dit 100% een oplichter.

Daarnaast is het belangrijk om zo veel mogelijk bewijzen te verzamelen. Noteer steeds alle gegevens die je van de oplichters kreeg, zoals telefoonnummers en namen. Neem eventueel screenshots van de vervalste mails, links en website. Met deze bewijzen op zak kan je eenvoudig een aangifte doen bij de politie en een proces-verbaal laten opstellen.

Tot slot, geef nooit persoonlijke codes door zoals je pincode of responscode. De bank zal deze codes immers nooit vragen via welk kanaal dan ook. Wees in het algemeen niet te naïef. Een bericht dat te mooi is om waar te zijn, zal dit meestal ook zijn. Daarnaast spelen phishers vaak in op het gevoel dat het snel moet gaan. Wees dus alert voor berichten waar een zekere urgentie achter zit. Geloof niet blindelings in elke mail of sms, maar geloof ook niet dat het jou nooit zou overkomen. Wees op je hoede en dubbelcheck!

Komt u tijdens het surfen op het internet een verdacht bericht tegen, aarzel dan zeker niet om dit bericht door te sturen naar verdacht@safeonweb.be. Zij controleren de links en bijlages van deze doorgestuurde berichten waarbij ze in staat zijn om verdachte links te laten blokkeren. Op die manier zijn minder oplettende internetgebruikers die op de link geklikt hebben, ook beschermd. Door snel te ageren, verkleint de kans dat cybercriminelen slachtoffers maken. Een gewaarschuwd man is er twee waard.

Indien u na het lezen van dit artikel nog vragen hebt omtrent phishing, aarzel dan niet om ons te contacteren via joost.peeters@studio-legale.be, simon.geens@studio-legale.be of 03 216 70 70.

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

[2] https://www.vrt.be/vrtnu/a-z/pano/2021/pano-s2021a7/.

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

[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

————————————————————————————————

Le phishing : le nouveau cambriolage en 2021?

34. *000. 000 euros.[1] C'est le montant total que les phishers ont pu voler en 2020. Qu'est-ce que le phishing et comment ces cybercriminels opèrent-ils ? Serai-je remboursé si je suis victime d'une escroquerie et comment reconnaître les faux e-mails ? Nous avons fait quelques recherches pour vous.*

Phishing?

Le phishing est une forme de cybercriminalité dans laquelle la victime potentielle est approchée par courrier électronique, par SMS, par les médias sociaux ou par téléphone. L'escroc se fait passer pour quelqu'un d'autre dans le but d'accéder aux données confidentielles des victimes. Elle est similaire à la fraude sur Internet, sauf que l'auteur ne manipule pas des données, mais des personnes. C'est un méthode psychologique pour gagner la confiance de la victime. Les phishers travaillent de manière très ingénieuse et anticipent habilement les événements actuels. Des messages d'une banque, d'une entreprise technologique ou d'un service postal indiquant qu'un colis vous attend, la probabilité que vous ayez reçu l'un de ces messages est très élevée.

Le phénomène du phishing ou de « l'hameçonnage" des données sensibles telles que les mots de passe et les coordonnées bancaires ou de cartes de crédit, a connu une croissance exponentielle ces dernières années. En 2020, pas moins de 3. 200. 000 messages suspects ont été transmis au Centre de cybersécurité de Belgique (CCB). Au cours du premier semestre de l'année dernière, les services de police ont établi 3 438 rapports officiels sur le phishing. C'est quatre fois plus élevé que l'année précédente. Mais ce n'est que la partie visible de l'iceberg,

selon le ministère public.[2]

Il y a plusieurs raisons à cela. Tout d'abord, le nombre de messages d'hameçonnage augmentent de manière exponentielle, ce qui signifie que le ministère public ne peut tout simplement plus traiter l'afflux de dossiers. Cela ressemble presque à un effet secondaire négatif de la crise du Corona, maintenant que les contacts se font de plus en plus par voie numérique. Compte tenu des nombreuses victimes et des ressources humaines et financières limitées du ministère de la justice, la probabilité que les délinquants soient arrêtés est plutôt faible.

En outre, l'anonymat de l'auteur des faits est un facteur explicatif important. Bien à l'abri derrière son écran d'ordinateur, un cybercriminel peut voler des milliers de personnes en même temps, tout en échappant au radar de la loi, car dans de nombreux cas, ils sont incapables de découvrir l'identité de la personne qui envoie de faux messages ou crée un faux site web. Les auteurs de ces actes s'imaginent qu'ils bénéficient de l'impunité.

Enfin, le phishing est un jeu d'enfant. Il n'est pas nécessaire d'être un magicien de l'informatique pour faire du phishing. Il s'agit simplement de gagner la confiance des victimes afin d'extraire des informations sensibles et de voler de l'argent.

Comment ces cybercriminels opèrent-ils?

C'est assez simple. Le phishing a souvent une organisation structurée. Au sommet de la pyramide se trouvent les experts en informatique qui créent des logiciels permettant d'élaborer des sites et des e-mails de phishing crédibles. En piratant des sites web où des personnes se sont inscrites, les fraudeurs s'emparent de données proposées dans les groupes de discussion fermés via des marchés en ligne. Les phishers achètent les données qui proviennent des logiciels et choisissent leurs victimes dans cette liste. De cette manière, les phishers peuvent souvent envoyer des messages à des milliers de personnes en même temps. En bas, ce sont les mules financières. L'argent des victimes que les phishers volent finit sur leurs comptes. En d'autres termes, il s'agit d'une sorte de tactique de diversion pour les autorités judiciaires, car de cette façon, non seulement les chefs de bande restent souvent hors de portée des enquêteurs, mais les phishers ne peuvent guère être retrouvés non plus.

Serai-je remboursé?

La question la plus importante pour les victimes est peut-être : vais-je récupérer mon argent ? Il est essentiel que les victimes agissent rapidement. Si vous

estimez qu'une transaction est finalement suspecte, contactez immédiatement votre banque. Ils peuvent faire bloquer l'accès à vos comptes. La probabilité que vous soyez dans les temps semble plus faible à partir du moment où l'ordre a été donné et que l'argent a définitivement quitté la banque. C'est pourquoi les banques travaillent ensemble pour faire bloquer les comptes le plus rapidement possible. Dès qu'une banque est informée d'un cas de phishing, la banque de la victime contacte la banque de la mule. En d'autres termes, la banque à laquelle l'argent est transféré. Ils tenteront de bloquer les fonds et de les récupérer par la suite.

Si cela ne fonctionne pas et que l'argent a déjà disparu, il existe une possibilité d'indemnisation par votre banque. Ce dernier procédera à un équilibre entre les intérêts en présence pour déterminer si vous pouvez être tenu responsable ou non. Pour cela, la banque utilise la notion de "négligence grave".[3] Ils examineront chaque situation pour déterminer quelle technique de fraude a été utilisée et si les clients ont été trop négligents en partageant leurs données personnelles – bien que sous pression et de bonne foi – avec un cybercriminel. Dans tous les cas, la charge de la preuve incombe à la banque et ce n'est pas à vous de prouver que vous n'avez pas été négligent.

La notion de "négligence grave" fait l'objet d'un débat animé, car la loi ne définit pas clairement ce qui doit être considéré comme une "négligence grave" et ce qui ne doit pas l'être. Test Achats[4] estime que les banques utilisent ce concept en permanence pour éviter de rembourser l'argent. Parmi les exemples de "négligence grave", citons le fait de ne pas bloquer sa carte bancaire, de ne pas conserver la carte avec le code ou de ne pas la confier à quelqu'un. Mais il est très difficile de tracer une ligne générale ici. Dans la pratique, beaucoup de banques remboursent le client dans de nombreux cas.[5]

Si la banque déclare que vous êtes entièrement responsable et que vous pensez être la victime, n'hésitez pas à porter votre conflit devant l'Ombudsfin[6], le service de médiation des litiges financiers. Il s'agit d'une institution indépendante qui peut servir de médiateur dans les litiges relatifs aux transactions frauduleuses et aux remboursements entre la victime et la banque.

Comment reconnaître les faux messages?

Les phishers sont très inventifs et inventent régulièrement de nouvelles astuces pour escroquer les gens de leur argent ou de leurs données. En outre, les méthodes d'escroquerie sont également de plus en plus difficiles à reconnaître. Distinguer les faux e-mails des messages fiables semble presque impossible. Nous avons répertorié, ci-dessous, un certain nombre de conseils pour évaluer si vous

pouvez faire confiance à un message.

Vous doutez qu'un message soit suspect ? Répondez ensuite brièvement à ces questions pour vous-même :[7]

- Est-ce inattendu?
- C'est urgent?
- Connaissez-vous l'expéditeur?
- Trouvez-vous la question étrange?
- Sur quoi le lien vous amène-t-il à cliquer ? Conseil: survolez le lien et voyez où il vous mène. Il est préférable de ne pas ouvrir un lien suspect.
- Connaissez-vous l'expéditeur?
- S'adresse-t-on à vous personnellement?
- Le message contient-il de nombreuses erreurs de langage ?
- Le message est-il dans votre Spam?
- Est-ce que quelqu'un essaie de vous rendre curieux?

Vous ne vous sentez pas à l'aise avec une transaction que vous avez effectuée? Contactez Card Stop dès que possible pour faire bloquer votre carte. Vous pouvez le faire en appelant le 070 344 344. Veuillez noter que Card Stop n'appelle jamais les gens. Si quelqu'un se fait passer pour un employé de Card Stop au téléphone, cette personne est à 100% un fraudeur.

Il est également important de rassembler autant de preuves que possible. Notez toujours tous les détails que vous avez reçus des escrocs, tels que les numéros de téléphone et les noms. Si nécessaire, faites des captures d'écran des courriels, des liens et du site Web falsifiés. Avec ces preuves en poche, vous pouvez facilement porter plainte auprès de la police et faire établir un rapport officiel.

Enfin, ne donnez jamais de codes personnels tels que votre numéro PIN ou votre code de réponse. La banque ne demandera jamais ces codes par quelque canal que ce soit. En général, ne soyez pas trop naïfs. Un message qui est trop beau pour être vrai l'est généralement. En outre, les phishers jouent souvent avec l'impression que les choses doivent se passer rapidement. Soyez donc attentif aux messages qui ont un caractère d'urgence. Ne croyez pas aveuglément chaque e-mail ou SMS, mais ne croyez pas non plus que cela ne vous arrivera jamais. Soyez sur vos gardes et vérifiez à nouveau !

Si vous tombez sur un message suspect en surfant sur Internet, n'hésitez pas à le transmettre à verdacht@safeonweb.be. Ils vérifient les liens et les pièces jointes de ces messages transférés et sont capables de bloquer les liens suspects. De cette façon, les internautes moins attentifs qui ont cliqué sur le lien sont

également protégés. En agissant rapidement, on réduit les chances que les cybercriminels fassent des victimes. Un homme avertit en vaut deux.

Si vous avez encore des questions sur le phishing après avoir lu cet article, n'hésitez pas à nous contacter via joost.peeters@studio-legale.be, simon.geens@studio-legale.be ou 03 216 70 70.

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

[2] https://www.vrt.be/vrtnu/a-z/pano/2021/pano-s2021a7/.

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

[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

————————————————————————————————

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.

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.

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'. Testaankoop[4] 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 Ombudsfin[6], 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]

- Is it unexpected?
- Is it urgent?

- Do you know the sender?
- Do you find the question strange?
- 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.
- Are you addressed personally?
- Does the message contain many language errors?
- Is the message in your Spam?
- 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 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.

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

[2] https://www.vrt.be/vrtnu/a-z/pano/2021/pano-s2021a7/.

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

[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

————————————————————————————————

Phishing: der neue Einbruch im Jahr 2021?

34.000.000 Euro.[1] Das ist der Gesamtbetrag, den Phisher im Jahr 2020 stehlen konnten. Was ist Phishing und wie gehen diese Cyberkriminellen vor? Bekomme ich mein Geld zurück, wenn ich betrogen wurde und wie erkenne ich gefälschte E-Mails? Wir haben es für Sie herausgefunden.

Phishing?

Phishing ist eine Form der Cyberkriminalität, bei der das potenzielle Opfer per E-Mail, Textnachricht, soziale Medien oder Telefon angesprochen wird. Der Betrüger gibt sich als eine andere Person aus, um an die vertraulichen Daten der Opfer zu gelangen. Es ist ähnlich wie beim Internet-Betrug, nur dass der Täter nicht Daten, sondern Menschen manipuliert. Es ist eine Form der Psychologie, auf diese Weise das Vertrauen des Opfers zu gewinnen. Phisher arbeiten sehr raffiniert und antizipieren geschickt aktuelle Ereignisse. Nachrichten von einer Bank, einem Technologieunternehmen oder einem Postdienst, die besagen, dass ein Paket auf Sie wartet, die Wahrscheinlichkeit, dass Sie eine dieser Nachrichten erhalten haben, ist sehr hoch.

Das Phänomen des Phishings oder “Angelns” nach sensiblen Daten wie Passwörtern und Bank- oder Kreditkartendaten hat in den letzten Jahren exponentiell zugenommen. Im Jahr 2020 wurden nicht weniger als 3.200.000 verdächtige Nachrichten an das Centre for Cybersecurity Belgium (CCB) weitergeleitet. In der ersten Hälfte des vergangenen Jahres erstellten die Polizeidienststellen 3.438 offizielle Berichte über Phishing. Eine Vervierfachung

im Vergleich zum Vorjahr. Doch das ist nur die Spitze des Eisbergs, so die Staatsanwaltschaft.[2]

Dafür gibt es verschiedene Gründe. Zum einen steigt die Zahl der Phishing-Nachrichten exponentiell an, so dass die Staatsanwaltschaft die Flut an Dateien einfach nicht mehr verarbeiten kann. Es scheint fast ein unangenehmer Nebeneffekt der Corona-Krise zu sein, dass Kontakte nun zunehmend digital geknüpft werden. Angesichts der vielen Opfer und der begrenzten personellen und finanziellen Ressourcen der Justiz ist die Chance, dass die Täter gefasst werden, eher gering.

Darüber hinaus ist die Anonymität des Täters ein wichtiger Erklärungsfaktor. Sicher hinter seinem Computerbildschirm kann ein Cyberkrimineller unter dem Radar des Gesetzes Tausende Menschen gleichzeitig ausrauben, da sie in vielen Fällen nicht in der Lage sind, die Identität der Person zu ermitteln, die falsche Nachrichten verschickt oder eine gefälschte Website einrichtet. Die Täter glauben, dass sie straffrei bleiben.

Schließlich ist Phishing ein Kinderspiel. Sie müssen kein Computergenie sein, um Phishing zu betreiben. Es geht einfach darum, das Vertrauen der Opfer zu gewinnen, um sensible Informationen zu extrahieren und Geld zu stehlen.

Wie arbeiten diese Cyberkriminellen?

Ganz einfach. Phishing hat oft eine strukturierte Organisation. An der Spitze der Pyramide stehen die IT-Experten, die Softwareprogramme erstellen, mit denen sie glaubwürdige Phishing-Seiten und -E-Mails erstellen können. Durch das Hacken von Webseiten, auf denen sich Menschen registriert haben, gelangen die Betrüger an Daten, die in geschlossenen Chatgruppen über Online-Marktplätze angeboten werden. Phisher kaufen die Daten, die von den Softwareprogrammen stammen, und wählen ihre Opfer aus dieser Liste aus. Auf diese Weise können Phisher oft Tausende Personen gleichzeitig anschreiben. Ganz unten sind die Geldesel. Das Geld der Opfer, das die Phisher stehlen, landet auf deren Konten. Also eine Art Ablenkungsmanöver für die Justizbehörden, denn so bleiben nicht nur die Bandenchefs für die Ermittler oft unauffindbar, sondern auch die Phisher können kaum aufgespürt werden.

Bekomme ich mein Geld zurück?

Die vielleicht wichtigste Frage für die Opfer ist: Bekomme ich mein Geld zurück? Es ist wichtig, dass Opfer schnell handeln. Wenn Ihnen eine Transaktion doch verdächtig vorkommt, wenden Sie sich sofort an Ihre Bank. Sie können den Zugriff auf Ihre Konten sperren lassen. Die Chance, dass Sie rechtzeitig sind,

scheint kleiner zu sein, da das Geld ab dem Zeitpunkt der Auftragserteilung definitiv die Bank verlassen hat. Deshalb arbeiten die Banken zusammen, um Konten so schnell wie möglich sperren zu lassen. Sobald eine Bank über einen Phishing-Fall informiert wird, nimmt die Bank des Opfers Kontakt mit der Bank des Geldkuriers auf. Mit anderen Worten: die Bank, an die das Geld überwiesen wird. Sie werden versuchen, die Gelder zu sperren und sie anschließend wieder einzuziehen.

Wenn dies nicht funktioniert und das Geld bereits verschwunden ist, besteht die Möglichkeit einer Entschädigung durch Ihre Bank zu bekommen. Dieser wird eine Interessenabwägung vornehmen, ob Sie haftbar gemacht werden können oder nicht. Hierfür verwendet die Bank die Kennzahl "große Fahrlässigkeit"[3]. Sie werden jede Situation prüfen, um zu sehen, welche Betrugstechnik verwendet wurde und ob die Kunden zu unvorsichtig waren, indem sie ihre persönlichen Daten – wenn auch unter Druck und in gutem Glauben – an einen Cyberkriminellen weitergaben. In jedem Fall liegt die Beweislast bei der Bank und es liegt nicht an Ihnen, zu beweisen, dass Sie nicht fahrlässig waren.

Die Figur der "großen Fahrlässigkeit" ist Gegenstand heftiger Diskussionen, da das Gesetz nicht eindeutig definiert, was als "große Fahrlässigkeit" zu verstehen ist und was nicht. Testaankoop[4] ist der Meinung, dass Banken dieses Konzept immer wieder nutzen, um die Rückzahlung zu vermeiden. Beispiele für "große Fahrlässigkeit" sind, dass Sie Ihre Bankkarte nicht sperren oder die Karte nicht zusammen mit dem Code aufbewahren oder sie niemandem anvertrauen. Aber es ist sehr schwierig, hier eine allgemeine Linie zu ziehen. In der Praxis erstatten viele Banken dem Kunden in vielen Fällen Geld zurück.[5]

Wenn die Bank die volle Verantwortung übernimmt und Sie sich als Opfer fühlen, zögern Sie nicht, Ihren Konflikt an Ombudsfin[6], die Schlichtungsstelle für Finanzstreitigkeiten, zu richten. Dies ist eine unabhängige Institution, die bei Streitigkeiten über betrügerische Transaktionen und Erstattungen zwischen dem Opfer und der Bank vermitteln kann.

Wie erkenne ich falsche Meldungen?

Phisher sind sehr erfinderisch und erfinden regelmäßig neue Tricks, um Menschen um Geld oder Daten zu betrügen. Außerdem werden die Betrugsmethoden immer schwieriger zu erkennen. Die Unterscheidung zwischen falschen E-Mails und zuverlässigen Nachrichten scheint fast unmöglich. Im Folgenden haben wir eine Reihe von Tipps aufgelistet, um zu beurteilen, ob Sie einer Nachricht vertrauen können.

Zweifeln Sie daran, dass eine Meldung verdächtig ist? Dann beantworten Sie diese Fragen kurz für sich selbst:[7]

- Ist es unerwartet?
- Ist es dringend?
- Kennen Sie den Absender?
- Finden Sie die Frage seltsam?
- Wohin führt der Link, den Sie anklicken sollen? Tipp: Fahren Sie mit dem Mauszeiger über den Link und sehen Sie, wohin er Sie führt. Öffnen Sie einen verdächtigen Link am besten nicht.
- Werden Sie persönlich angesprochen?
- Enthält die Nachricht viele Sprachfehler?
- Ist die Nachricht in Ihrem Spam?
- Versucht jemand, Sie neugierig zu machen?

Riecht es nach einem von Ihnen getätigten Geschäft? Wenden Sie sich so schnell wie möglich an Card Stop, um Ihre Karte sperren zu lassen. Sie können dies unter der Nummer 070 344 344 tun. Bitte beachten Sie, dass Card Stop niemals Personen anrufen wird. Wenn jemand am Telefon vorgibt, ein Mitarbeiter von Card Stop zu sein, ist diese Person 100% sicher ein Betrüger.

Es ist auch wichtig, so viele Beweise wie möglich zu sammeln. Notieren Sie sich immer alle Details, die Sie von den Betrügern erhalten haben, wie z. B. Telefonnummern und Namen. Machen Sie ggf. Screenshots von den gefälschten E-Mails, Links und der Website. Mit diesen Beweisen können Sie problemlos eine Anzeige bei der Polizei erstatten und einen offiziellen Bericht erstellen lassen.

Geben Sie schließlich niemals persönliche Codes wie Ihre PIN-Nummer oder Ihren Antwortcode an. Die Bank wird niemals auf irgendeinem Weg nach diesen Codes fragen. Im Allgemeinen sollten Sie nicht zu naiv sein. Eine Nachricht, die zu schön ist, um wahr zu sein, ist es meistens auch. Darüber hinaus spielen Phisher oft mit dem Gefühl, dass es schnell gehen muss. Seien Sie also wachsam für Nachrichten, die eine gewisse Dringlichkeit hinter sich haben. Glauben Sie nicht blind jeder E-Mail oder Textnachricht, aber glauben Sie auch nicht, dass es Ihnen nie passieren wird. Seien Sie auf der Hut und prüfen Sie doppelt!

Wenn Sie beim Surfen im Internet auf eine verdächtige Nachricht stoßen, zögern Sie nicht, sie an verdacht@safeonweb.be weiterzuleiten. Sie prüfen die Links und Anhänge dieser weitergeleiteten Nachrichten und sind in der Lage, verdächtige Links zu blockieren. Auf diese Weise werden auch weniger aufmerksame Internetnutzer, die auf den Link geklickt haben, geschützt. Durch schnelles Handeln wird die Chance, dass Cyberkriminelle Opfer finden, verringert. Eine

Warnung ist zwei wert.

Wenn Sie nach dem Lesen dieses Artikels noch Fragen zum Thema Phishing haben, zögern Sie nicht, uns über joost.peeters@studio-legale.be, simon.geens@studio-legale.be oder 03 216 70 70 zu kontaktieren.

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

[2] https://www.vrt.be/vrtnu/a-z/pano/2021/pano-s2021a7/.

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

[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