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.

[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 geinformeerd.

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.

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

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

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

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

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]

1. Est-ce inattendu?
2. C'est urgent?
3. Connaissez-vous l'expéditeur?
4. Trouvez-vous la question étrange?
5. 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.
6. S'adresse-t-on à vous personnellement?

[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

7. Le message contient-il de nombreuses erreurs de langage ?
8. Le message est-il dans votre Spam?
9. 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.