Le phishing, ça se joue dans les détails! Installez l'extension de navigateur Safeonweb et ne vous faites plus jamais avoir

La campagne de cette année donne aux internautes de nouveaux outils pour assurer leur sécurité en ligne

BRUXELLES, 16 OCTOBRE 2023
Le 16 octobre, le Centre pour la cybersécurité Belgique[1] (CCB), Febelfin et la Cyber Security Coalition lancent une nouvelle campagne de sensibilisation sur le phishing avec le slogan: « *Le phishing, ça se joue dans les détails !* » Cette forme d'escroquerie en ligne est en recrudescence et continue à faire nombre de victimes qu'il s'agisse de particuliers, d'entreprises ou d'organisations.

Quelques chiffres sur le phishing

- En 2022, un total de 39,8 millions d'euros ont été dérobés par le biais du phishing, ce qui représente une augmentation par rapport à l'année précédente (2021: 25 millions d'euros). Cela est principalement dû à l'augmentation considérable du nombre de messages de phishing envoyés.
- 69% des Belges ont reçu au moins un message de phishing au cours des 6 derniers mois (*source*: Febelfin & Indiville, mars 2023)
- 8% des Belges n'ont jamais entendu parler de phishing. La tranche d'âge la plus âgée obtient de meilleurs résultats à cet égard: 4% n'ont jamais entendu parler de phishing, ce qui représente une amélioration par rapport à 2022 (7%). Bien qu'il y ait une légère amélioration par rapport à 2021 (24%) et 2022 (30%), le nombre de jeunes qui ne savent pas ce qu'est le phishing est trop élevé (23%).
- 8% des Belges disent avoir été victimes de phishing. Chez les jeunes, ce pourcentage est plus élevé (12%).
- Seuls 62% des victimes belges d'hameçonnage connaissaient les mesures à prendre.

Source: Dossier d'informations: Don't be fooled by a 'phish' (Febelfin.be)

[1] Le CCB est l'autorité nationale de cybersécurité en Belgique et est placé sous l'autorité du Premier ministre.

- De janvier à septembre 2023, plus de 7 millions de messages ont déjà été transmis à suspect@safeonweb.be, ce qui dépasse le chiffre record de 2022, année au cours de laquelle nous avons reçu pas moins de 6 millions de messages.
- Cela représente une moyenne de 26 425 messages par jour.
- Dans un récent sondage commandé par le Centre pour la Cybersécurité Belgique (en septembre 2023), 28% des personnes interrogées ont déclaré ne pas savoir comment reconnaître un faux site web.
- 78% déclarent qu'ils ne cliqueraient jamais sur un lien suspect, alors que 22% le feraient peut-être.
- 57% des répondants estiment que la probabilité qu'ils soient un jour victime d'hameçonnage est élevée.
- Plus de 600 partenaires s'associent chaque année à la campagne Safeonweb (CCB). Ces dernières années, celle-ci nous a permis de toucher la moitié de la population belge (+18 ans).

Source: Safeonweb, 2023

Pourquoi n'est-il pas possible d'éradiquer le phishing?

Le phishing n'est pas un phénomène nouveau. La constante dans l'évolution de ce phénomène est que les fraudeurs cherchent toujours à obtenir des données (bancaires) par le biais de divers canaux tels que les mails, le téléphone, les courriers, le SMS, les médias sociaux ou les outils de messagerie comme WhatsApp. Dans ce type d'escroqueries financières, les criminels se font souvent passer pour des organisations ou institutions dignes de confiance (banques, administrations ou autres services publics...).

Le message envoyé contient un lien vers un faux site web, où la victime est invitée à saisir ses codes bancaires personnels. Lorsque les fraudeurs ont mis la main sur des codes bancaires personnels, ils peuvent effectuer des transactions au nom de la victime.

> *Les messages de phishing sont un véritable fléau. Ils circulent massivement en permanence et ne cessent de faire des victimes. Pourquoi n'est-il pas possible de se débarrasser de ce phénomène? Cela peut s'expliquer par plusieurs raisons. Il est assez facile d'attiser l'instinct humain en utilisant la curiosité ou la peur. Nous ne pouvons pas résister à une offre alléchante. Les hameçonneurs capitalisent sur ces caractéristiques typiquement humaines. Ils essaient d'approcher et de convaincre leurs victimes par une série d'artifices. C'est précisément la signification du terme « ingénierie sociale ».*
>
> *En outre, les messages de phishing sont de plus en plus difficiles à repérer: ils ne contiennent plus que rarement des fautes d'orthographe, sont formatés de manière professionnelle, renvoient à des sites web très convaincants, etc. Les cybercriminels se sont professionnalisés, ce qui nous fait dire que l'avenir proche n'est pas forcément radieux. Bien que les progrès liés au développement de l'IA ouvrent de nombreuses perspectives positives, les escrocs ont également bien compris l'opportunité d'utiliser les différentes applications pour envoyer des messages convaincants, attrayants et personnalisés.*

Miguel De Bruycker, Directeur général du Centre pour la Cybersécurité Belgique

Le phishing, ça se joue dans les détails !

Il n'est toutefois pas impossible de démasquer les messages et les sites de phishing. Tout se joue dans les détails. Pour être sûr de ne pas cliquer sur le site d'un escroc, vous devez apprendre à bien lire l'URL du site. Comment s'y prendre?

Passez votre souris sur le lien. Le nom de domaine, c.-à-d. le mot qui précède .be, .com, .eu, .org, ... et la toute première barre oblique "/", est-il vraiment le nom de l'organisation? Dans ce cas, vous pouvez être sûr que vous vous rendez sur le vrai site web. Attention, en revanche, si vous voyez quelque chose d'autre à cet endroit! Une combinaison étrange? Ou le nom de domaine que vous attendez, mais avec une légère différence?

Un exemple:

- Pour www.safeonweb.be/tips, le nom de domaine est **safeonweb**. Vous êtes ici sur le bon site.
- Sur le lien www.safeonweb.tips.be/safeonweb, le nom de domaine est "**tips**" et vous êtes dirigé vers un autre site web.

Les escrocs peuvent utiliser des URL légèrement différentes. Examinez donc toujours très attentivement l'URL avant de cliquer dessus. Vous avez des doutes? Dans ce cas, ne cliquez pas sur un lien contenu dans un message, mais allez vous-même sur le site web en tapant l'URL que vous connaissez et que vous utilisez habituellement dans la barre de votre navigateur.

Le Centre pour la Cybersécurité Belgique lance l'extension de navigateur Safeonweb

Etant donné que la lecture et la compréhension correcte des URL demeurent une difficulté majeure pour bon nombre de personnes, nous lançons un nouvel outil: l'extension de navigateur Safeonweb. Celle-ci doit vous aider à évaluer la fiabilité de tout site web visité. L'extension attribue un niveau de confiance à chaque site: élevé, moyen ou faible. Ce niveau est basé sur des facteurs connus concernant le domaine du site web, son propriétaire et le niveau de certification obtenu auprès d'une autorité de certification.

La campagne a pour objectif de stimuler le comportement suivant: l'installation de l'extension Safeonweb dans votre navigateur. Celle-ci doit vous alerter lorsque vous visitez un site web non sécurisé sur lequel il est dangereux de saisir vos données.

Voir tous les détails sur l'installation et l'utilisation de ce nouvel outil sur **www.safeonweb.be**.

Outils Safeonweb pour surfer en toute sécurité

À côté de l'extension de navigateur, Safeonweb met déjà à disposition 3 autres outils :

1. **Adresse électronique: suspect@safeonweb.be**

Transmettez le message suspect à suspect@safeonweb.be. Sur la base de tous les messages transmis à suspect@safeonweb.be, nous examinons les liens suspects. Si un internaute moins attentif clique sur ce lien, il recevra un avertissement clair l'invitant à ne pas se rendre sur cette page.

2. **L'application Safeonweb**

Nous recueillons des informations sur les messages suspects les plus courants et les partageons via l'application Safeonweb. Cela vous permet d'être rapidement informé·e lorsque des messages suspects sont en circulation. Vous trouverez l'application Safeonweb dans les magasins d'applications officiels (App Store et Google Play Store).

3. **L'apprentissage en ligne Safeonweb**

Apprenez à repérer les messages suspects en 10 minutes: consultez surfersanssoucis.safeonweb.be

Febelfin met en place une véritable « *Hacker Hotline* »

Grâce à la *Hacker Hotline*, un *escape game* mobile, Febelfin souhaite sensibiliser les jeunes de manière ludique aux dangers liés à la fraude en ligne et à l'appât du gain rapide d'argent. Cela doit également les aider à s'armer contre ces pratiques. Les joueurs sont mis au défi d'être plus malins que le cybercriminel ("hameçonneur") … Ce jeu est un complément idéal à cette nouvelle campagne de sensibilisation nationale.

> *La "Hacker Hotline" est un escape game mobile par lequel Febelfin vise les jeunes, nos partenaires, les écoles et les événements afin de sensibiliser aux formes de fraude en ligne telles que le phishing. Le jeu permet d'explorer les techniques utilisées par les fraudeurs pour piéger leurs victimes et d'apprendre à s'armer contre ce type de fraude. Si vous parvenez à vous échapper du bus, vous disposerez de tous les outils nécessaires pour naviguer en ligne en toute sécurité dans la vie réelle. En même temps, vous apprendrez des concepts fondamentaux tels que l'authentification à 2 facteurs ou ce que l'on entend par mot de passe fort.*
>
> **Karel Baert**, CEO Febelfin.

À qui s'adresse-t-il?
L'*escape game* s'adresse avant tout aux jeunes pour les sensibiliser aux dangers de l'appât du gain rapide d'argent et aux formes de fraude telles que le phishing et la fraude WhatsApp, entre autres. Le grand public peut aussi y participer et bénéficier de ce nouveau type de sensibilisation. La "Hacker Hotline" peut être utilisée par nos partenaires, les organisations, les associations ou les écoles qui souhaitent mettre en garde contre la fraude en ligne.

Faire campagne ensemble

Nous pourrons vaincre le phishing uniquement par la collaboration entre les autorités, la police, la justice, le secteur des télécommunications... C'est pourquoi le CCB, Febelfin et la Cyber Security Coalition, ainsi que plus de **600 partenaires**, ont uni leurs forces pour une nouvelle campagne de sensibilisation de grande envergure visant à informer et à mettre en garde. L'objectif est de parvenir à accroître la vigilance des internautes. Un citoyen vigilant en vaut deux et c'est l'objectif de cette campagne de sensibilisation.

La campagne vise à toucher le public le plus large possible sans aucune exception. Elle sera déployée sur de nombreux canaux: le message central sera diffusé publiquement par le biais de spots télévisés et dans les cinémas. La campagne sera également partagée sur les médias sociaux pour sensibiliser aux dangers du phishing. L'ensemble du matériel de la campagne peut être téléchargé sur le site https://safeonweb.be/fr/materiel-de-campagne.

> *Chaque année, le paysage des menaces ne cesse d'évoluer, exigeant une réponse collective de la part de l'industrie, du gouvernement, des universités et des citoyens. La campagne nationale de sensibilisation du CCB et de ses partenaires offre une plateforme essentielle pour que toutes les parties prenantes jouent un rôle actif dans le renforcement de nos défenses numériques.*
>
> **Séverine Waterbley**, présidente du SPF Économie et membre du conseil d'administration de la Cyber Security Coalition.

Plus d'informations?

N'hésitez pas à contacter le Centre pour la Cybersécurité Belgique ou Febelfin pour plus d'informations:

- Centre pour la cybersécurité Belgique:
  - 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 ou 02/507.68.31

Qui est qui?

A propos du Centre pour la cybersécurité Belgique

Le Centre pour la cybersécurité Belgique (CCB) est l'autorité nationale en matière de cybersécurité en Belgique. Le CCB supervise, coordonne et contrôle l'application de la stratégie belge en matière de cybersécurité. Le partage efficace de l'information permet aux entreprises, au gouvernement, aux fournisseurs de services essentiels et au public de se protéger de manière optimale. www.ccb.belgium.be

A propos de Febelfin

Febelfin ou la fédération du secteur bancaire belge. En tant que fédération sectorielle, nous sommes la voix des banques et représentons nos membres auprès des décideurs politiques, des régulateurs, des fédérations professionnelles et des groupes d'intérêt. Febelfin représente environ 245 institutions financières en Belgique. La mission de Febelfin: développer un secteur financier qui réponde aux besoins de la société.

A propos de la Cyber Security Coalition

La Cyber Security Coalition a pour mission de rendre la cybersécurité belge plus résiliente en construisant un écosystème de cybersécurité solide au niveau national. Il est nécessaire pour cela de réunir les compétences et l'expertise du monde universitaire, des entreprises et du gouvernement au sein d'une plateforme basée sur la confiance qui se concentre sur la promotion du partage d'informations, la coopération opérationnelle, la formulation de recommandations pour des politiques et des lignes directrices plus efficaces, et enfin la mise en œuvre de campagnes de sensibilisation conjointes pour les citoyens et les organisations. Plus de 1 200 représentants de nos 160 organisations membres participent à nos activités et contribuent à notre mission.