16 oct 2023 -10:29

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

Le 16 octobre, le Centre pour la cybersécurité Belgique (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 continue à faire nombre de victimes qu'il s'agisse de particuliers, d'entreprises ou d'organisations. Le CCB et Febelfin ont développé deux nouveaux outils pour mieux se prémunir contre cette forme de fraude.

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.
- 8% des Belges n'ont jamais entendu parler de phishing. Les jeunes surtout ignorent ce qu'est le phishing.

- 8% des Belges disent avoir été victimes de phishing. Chez les jeunes, ce pourcentage est encore 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)

- 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

"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? Il est assez facile d'attiser l'être humain vers 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 toute 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 démasquer: ils sont formatés de manière professionnelle, renvoient à des sites web très convaincants, etc. et les escrocs ont également bien compris l'opportunité d'utiliser les différentes applications d'IA pour envoyer des messages convaincants, attrayants et personnalisés.

"

Miguel De Bruycker
Directeur général du Centre pour la cybersécurité Belgique

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.

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 et c’est justement le slogan de la nouvelle campagne. Pour être sûr de ne pas surfer sur le site d’un escroc p.ex., il convient d’apprendre à bien lire l’URL d’un 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? Dans ce cas, méfiez-vous, car les escrocs peuvent l’exploiter pour vous tromper.

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.

Règle d’or: 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.

Un nouvel outil permettant d'identifier les sites web douteux

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 d'un site web. 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 (*call to action*): l'installation de l'extension Safeonweb dans votre navigateur. Celle-ci vous alerte lorsque vous visitez un site web non sécurisé sur lequel il est dangereux de saisir vos données.

Comment fonctionne l'extension de navigateur Safeonweb?

Lorsque vous surfez sur un site web, l'extension Safeonweb vous présente un indice de confiance – qui peut être vert, orange ou rouge – attribué au domaine du site.

L'extension Safeonweb a pour principal but de fournir des renseignements relatifs à la vérification de l'organisation et/ou du propriétaire du site web, plutôt que d'examiner le contenu de celui-ci. Il convient de souligner qu'un site web, même doté d'un indice de confiance élevé, peut être sujet à un piratage et héberger des logiciels malveillants. Il est donc important de toujours faire preuve de vigilance lorsque vous partagez ou signez en ligne. N'acceptez jamais une transaction (via itsme® ou votre lecteur de carte) à la demande d'une personne se présentant comme « un·e employé·e du helpdesk » ou un·e « employé·e de banque ».

Comment installer l'extension du navigateur?

Pour installer l'extension Safeonweb sur votre navigateur Chrome, suivez les étapes suivantes:

- Ouvrez le « Chrome Web Store ».
- Recherchez l'extension de navigateur Safeonweb et sélectionnez-la.
- Cliquez sur le bouton "Ajouter à Chrome".
- Dans la fenêtre contextuelle, cliquez sur le bouton « Ajouter une extension ».

- Sélectionnez l'icône en forme de pièce de puzzle situé dans le coin supérieur droit de votre navigateur et « épinglez » l'extension Safeonweb.
- L'icône Safeonweb apparaîtra à droite de la barre d'adresse. Sa couleur variera en fonction du niveau de confiance du site web que vous visitez.

Autres outils Safeonweb pour une navigation sécurisée

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

1. Adresse électronique: suspect@safeonweb.be
2. L'application Safeonweb: https://safeonweb.be/fr/safeonweb-app

3. L’apprentissage en ligne Safeonweb: https://surfersanssoucis.safeonweb.be/fr/

Febelfin vous met au défi avec la « Hacker Hotline »

Grâce à la *Hacker Hotline*, un *escape game* mobile, Febelfin souhaite sensibiliser les jeunes aux dangers de la fraude en ligne de manière ludique. Cela doit également les aider à s’armer contre ces pratiques. Les joueurs sont mis au défi d’être plus malins que le cybercriminel/phisher… Ce jeu est un complément idéal à cette nouvelle campagne de sensibilisation nationale car il n’est possible de gagner au jeu qu'en faisant attention aux détails.

A propos du jeu lui-même

Tout le monde peut être victime d’une fraude en ligne. Dans la « Hacker Hotline » vous êtes le point de contact des victimes de phishing et d’escroqueries. Votre tâche consiste à venir en aide – grâce à une ligne téléphonique et vidéo – aux personnes stressées, dans une course contre la montre. Le jeu devient encore plus excitant lorsque le pirate informatique apparaît soudainement dans le scénario.

La « Hacker Hotline » est une collaboration entre Febelfin et l'agence créative Hurae.

> "La « Hacker Hotline » est un escape game mobile par lequel Febelfin vise les jeunes, les 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 deux facteurs ou ce que l’on entend par mot de passe fort."

Karel Baert
CEO Febelfin.

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. 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. Les médias sociaux seront également utilisés 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 continue 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 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 en Belgique (CCB) est l’organe national de référence pour la cybersécurité en Belgique. Le CCB assure la supervision, la coordination et le suivi de la mise en œuvre de la stratégie belge en matière de cybersécurité. Un partage d’informations optimal permet aux entreprises, aux autorités publiques, aux fournisseurs de services essentiels et à la population de se protéger de manière adéquate. Pour plus d’informations, visitez www.ccb.belgium.be

A propos de Febelfin

Febelfin est la fédération représentative du secteur bancaire belge. En tant que fédération sectorielle, nous faisons entendre 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 est de développer un secteur financier au service de la société.

A propos de la Cyber Security Coalition

La mission de la Cyber Security Coalition est de renforcer la résilience de la Belgique en matière de cybersécurité en développant un écosystème robuste de cybersécurité à l’échelle nationale. Cet objectif peut être atteint en rassemblant les compétences et l’expertise du monde académique, du monde entrepreneurial et du gouvernement au sein d’une plateforme fondée sur la confiance. Cette plateforme se concentre sur la promotion du partage d’informations, la coopération opérationnelle, l’élaboration de recommandations pour des politiques et des directives plus efficaces, et la mise en œuvre de campagnes de sensibilisation conjointes à l’intention des citoyens et des organisations. Plus de 1 200 représentants de nos 160 organisations membres participent à nos activités et contribuent à notre mission.

Centre pour la Cybersécurité Belgique
Rue de la Loi 18
1000 Bruxelles
Belgique
http://www.ccb.belgium.be

Michele Rignanese
Porte-parole(NL/FR/E)
+32 (0)477 38 87 50
michele.rignanese@ccb.belgium.be

Katrien Eggers
Porte-parole(NL/FR/E)
+32 485 76 53 36
katrien.eggers@ccb.belgium.be