13 Juil 2023 -10:57

Cette année, 4,4 millions de messages de phishing ont déjà été transférés à Safeonweb

Au cours des six derniers mois, nous avons reçu près de 4,4 millions de messages dans la boîte mails de suspect@safeonweb.be, soit près de 2 millions de plus que les six premiers mois de 2022. Ces chiffres prouvent au moins deux choses : le phishing est loin d'être de l'histoire ancienne et la population a de plus en plus tendance à transmettre ces faux messages à Safeonweb.

Ces informations nous ont permis de bloquer plus de 320 000 liens suspects. Les internautes moins attentifs qui ont quand même cliqué sur ces liens ont été renvoyés vers une page d'avertissement et s'en sont donc sortis indemnes. Tous ces messages nous permettent de publier des alertes hebdomadaires sur notre site Internet et sur les médias sociaux. De cette manière, nous alertons au plus vite les victimes potentielles et continuons à informer les citoyens des derniers messages de phishing.

Nous constatons que les messages de phishing que nous recevons sont de plus en plus crédibles. Les messages sont à ce point bien rédigés qu'ils ressemblent très fort à des messages réels. Il est dès lors devenu très difficile de distinguer les vrais messages des faux. Nous remarquons que des messages de phishing consistent en fait en des copies ou des imitations de messages ou courriers d'information réels, avec insertion d'un ou de plusieurs faux liens. L'objectif est que vous fassiez confiance au contenu et que vous cliquiez sur une fausse page Internet.

Ne tombez plus dans le panneau !

Le moyen le plus efficace pour vérifier l'origine d'un message est d'analyser soigneusement les liens qu'il contient. Pour ce faire, il suffit de placer la souris sur le lien ou le bouton sans cliquer. L'adresse du site Internet auquel le lien renvoie ou l'URL s'affiche. Dans les exemples ci-dessous, vous voyez que cette adresse ne renvoie pas à une page d'Engie ou e-box.

C'est dans ce but que nous avons lancé avec la Cyber Security Coalition « Surfer sans soucis », une série de formations en ligne simples et accessibles sur la cybersécurité. Dans la première partie « Regarde où tu vas ! », vous apprenez à reconnaître les liens contenus dans les faux messages qui arrivent dans nos boîtes mails et sur nos téléphones portables.

Allez sur Surfer sans souci : https://surfersanssoucis.safeonweb.be/fr/modules/1

Quels messages suspects ont circulé entre janvier et juin ?

Nous avons surtout vu et revu beaucoup de grands classiques. Les messages annuels des autorités ou fournisseurs d'énergie à propos des primes, des impôts, des pensions, du pécule de vacances, etc. constituent une vaste source d'inspiration pour les cyberpirates. Ils se font passer pour le SPF Finances, le service des Pensions, les autorités wallonnes, Engie, et bien d'autres encore.

Les messages semblent provenir de My e-Box, Doccle ou MonEspace (Fédération Wallonie-Bruxelles). Et ces messages nous parviennent constamment.

Un autre type de messages qui peuvent nous rendre fous sont les sempiternels messages provenant soi-disant de sociétés de livraison. On vous demande en général avec insistance de payer des frais supplémentaires, de fournir des données manquantes ou de télécharger une application. Un scénario similaire est utilisé dans les messages qui semblent provenir des banques. Vous devez confirmer vos coordonnées pour obtenir un nouveau lecteur de carte ou encore pour continuer à avoir accès à votre compte bancaire. Ici aussi, il s'agit simplement de collecter vos données et de les utiliser à votre insu.

Astuce importante pour éviter les fraudes : ne cliquez pas sur un lien contenu dans un message

Allez sur la page de connexion de l'organisation (via votre navigateur et non le lien du message) pour vérifier les informations. Pour les exemples ci-dessus, vous irez donc sur la page de connexion de bpost ou d'un autre service de livraison, de votre fournisseur d'énergie, de votre e-box ou de Doccle. Si vous souhaitez vérifier les informations relatives à votre compte bancaire, passez par le site Internet ou l’application de votre banque.

Bien plus que du phishing

Les tentatives de phishing ont toujours pour objectif d'obtenir des données de la victime. Parfois, ces données sont utilisées immédiatement, par exemple pour piller votre compte bancaire. Dans d'autres cas, vos données sont conservées et revendues à d'autres cybercriminels qui, à leur tour, les utilisent pour commettre l’une ou l’autre escroquerie.

Ainsi, plusieurs scénarios sont utilisés pour convaincre la victime d’effectuer elle-même un virement. Le cybercriminel essaie d’obtenir votre confiance ou, au contraire, de vous inquiéter dans le seul but que vous effectuiez vous-même un virement. À titre d’exemple, citons la fraude à la relation, la fraude à l'investissement, la fraude via WhatsApp ou encore l’arnaque par sextortion.

Plus d'infos sur suspect@safeonweb.be ?

Plus d'infos sur suspect@safeonweb.be ?

Désormais, suivez aussi Safeonweb sur Instagram !

https://www.instagram.com/safeonweb.be/

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

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

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