44% des Belges ont transmis des signalements de phishing à l'adresse suspect@safeonweb.be

En 2024, les citoyens belges ont transmis plus de 9 millions de messages suspects à l'adresse suspect@safeonweb.be. Ce chiffre avait atteint un niveau record en 2023 avec 10 millions de signalements. Durant l'année écoulée, le Centre pour la Cybersécurité Belge (CCB) a reçu en moyenne 25 900 signalements par jour. Nous remercions chaleureusement tous les internautes qui contribuent ainsi à la sécurité en ligne. Grâce à leur vigilance, nous rendons Internet plus sûr.

Ces informations nous ont aidé à détecter et rediriger exactement 1 644 732 liens suspects. Notre système permet en effet de rediriger automatiquement les utilisateurs moins prudents vers une page d'avertissement, qui les protègent des tentatives d'escroquerie.

Une enquête réalisée par le Centre pour la Cybersécurité Belgique (Safeonweb, 12/2024) a montré que 44% des Belges transfèrent des messages à suspect@safeonweb.be (contre 39% en 2023). Cela montre que l'adresse électronique demeure un canal de communication privilégié. Il s'agit d'une source d'information essentielle que nous utilisons non seulement pour alimenter le bouclier anti-hameçonnage (le système BAPS), mais aussi pour avertir les citoyens.

Toutes ces notifications sont à la base des alertes ciblées concernant des messages de phishing en circulation publiées sur Safeonweb.be, Facebook, Instagram et X. Nous envoyons également ces alertes via l'application Safeonweb. En 2024, nous avons publié 81 alertes à propos des messages de phishing les plus fréquents à un moment donné.

Le phishing (ou hameçonnage): rien de neuf sous le soleil… ou pas?

Le phishing est resté l'une des méthodes d'attaque les plus utilisées et les plus évolutives de la cybercriminalité en 2024 (d'après le rapport *Threat Landscape* de l'ENISA, 2024).

À première vue, la plupart des messages de phishing ressemblent beaucoup à ceux de ces dernières années. D'une part, des messages semblant émaner de services publics, de la police, de banques, d'Itsme, etc. et, d'autre part, des offres dans la catégorie "trop beau pour être vrai", à savoir des promotions improbables ou des bonnes affaires ponctuelles, voire un "héritage perdu"… qui semble avoir refait surface dernièrement.

Les escrocs suivent toujours l'actualité de très près et l'utilisent pour donner de la crédibilité à leurs messages de phishing. Ainsi, chaque année, à l'approche des fêtes de fin d'année, nous voyons fleurir les messages concernant des promotions pour la Noël ou sur les livraisons de colis.

Nous constatons toutefois cinq changements

1. Le smishing et le vishing sont en augmentation

Le *smishing* (hameçonnage par SMS) et le *vishing* (hameçonnage par appel téléphonique) sont en augmentation. Les cybercriminels s'en servent pour obtenir directement des codes de vérification pour l'authentification à double facteur (2FA). Un exemple: les criminels appellent leur victime et se font passer pour un·e représentant·e de Cardstop pour l'assistance dans le cadre d'une transaction suspecte sur un

compte bancaire. L'escroc convainc la victime de transmettre les codes de vérification ou d'ouvrir Itsme pour procéder à l'authentification.

2. Davantage de phishing via les médias sociaux

Les plateformes telles que LinkedIn, Facebook, Instagram et WhatsApp sont de plus en plus utilisées pour diffuser des liens de phishing. Les principes sont les mêmes que pour le phishing par email ou par SMS.

3. Des attaques plus ciblées

Les fuites de données personnelles provenant de vols de données antérieurs facilitent la personnalisation des attaques et d'accroître leur niveau de crédibilité (que ce soit du phishing ou du smishing/vishing). Ces données volées permettent aux escrocs de gagner votre confiance. Lorsque vous recevez un appel d'un·e soi-disant employé·e de banque qui connaît votre nom, votre date de naissance et d'autres détails, cela vous incite à croire qu'il s'agit réellement d'un·e employé·e de banque.

4. L'IA et les *deepfakes* rendent le phishing plus crédible

Il ne fait aucun doute que les cybercriminels ont plus fréquemment recours à l'IA pour personnaliser les messages de phishing et les rendre plus convaincants. Dans la fraude au PDG (président) ou dans le *spear phishing*, un niveau de sophistication plus élevé est obtenu grâce aux *deepfakes* basés sur des images ou des voix manipulées p.ex. l'imitation de la voix du PDG de l'entreprise. Si de telles pratiques sont certainement possibles à l'heure actuelle, nous n'avons pas encore pu détecter d'exemples concrets.

5. Https n'est pas une garantie de sécurité

Les criminels utilisent de plus en plus les certificats SSL pour donner une apparence de légitimité à leurs liens de phishing. Attention donc: la présence du "https" ne garantit plus automatiquement la sécurité d'un site web. Un certificat SSL n'est pas une preuve absolue de fiabilité (Voir à ce sujet l'article https://safeonweb.be/fr/blog/un-site-internet-https-est-toujours-sur-vrai-ou-faux).

Bouclier anti-hameçonnage belge - Belgian Anti-Phishing Shield (BAPS)

Ce bouclier anti-hameçonnage protège les citoyens de notre pays contre les cybercriminels. C'est la pièce maîtresse du Centre pour la Cybersécurité en Belgique (CCB). Cette technologie de pointe nous place, en tant que petit pays, parmi les leaders mondiaux absolus.

Comment cela fonctionne-t-il?

1. Le Centre pour la Cybersécurité en Belgique (CCB) reçoit des informations sur des sites web potentiellement malveillants lorsque des internautes transmettent des messages suspects à suspect@safeonweb.be.

2. Les pièces jointes et autres liens sont ensuite extraits des messages suspects. Les URL sont également extraites des captures d'écran et des codes QR.

3. Le système analyse l'URL/le lien/la pièce jointe. S'il s'avère qu'il s'agit d'un site malveillant, il est répertorié et envoyé à nos partenaires (Fournisseurs d'accès Internet (FAI), Google Safe Browsing et Microsoft SmartScreen).

4. Lorsqu'un·e internaute clique sur un lien menant à un site malveillant, le FAI en question compare la requête DNS avec la liste des sites malveillants.

5. L'utilisateur/-rice est alors redirigé·e vers une page d'avertissement et ne peut plus visiter le site malveillant.

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