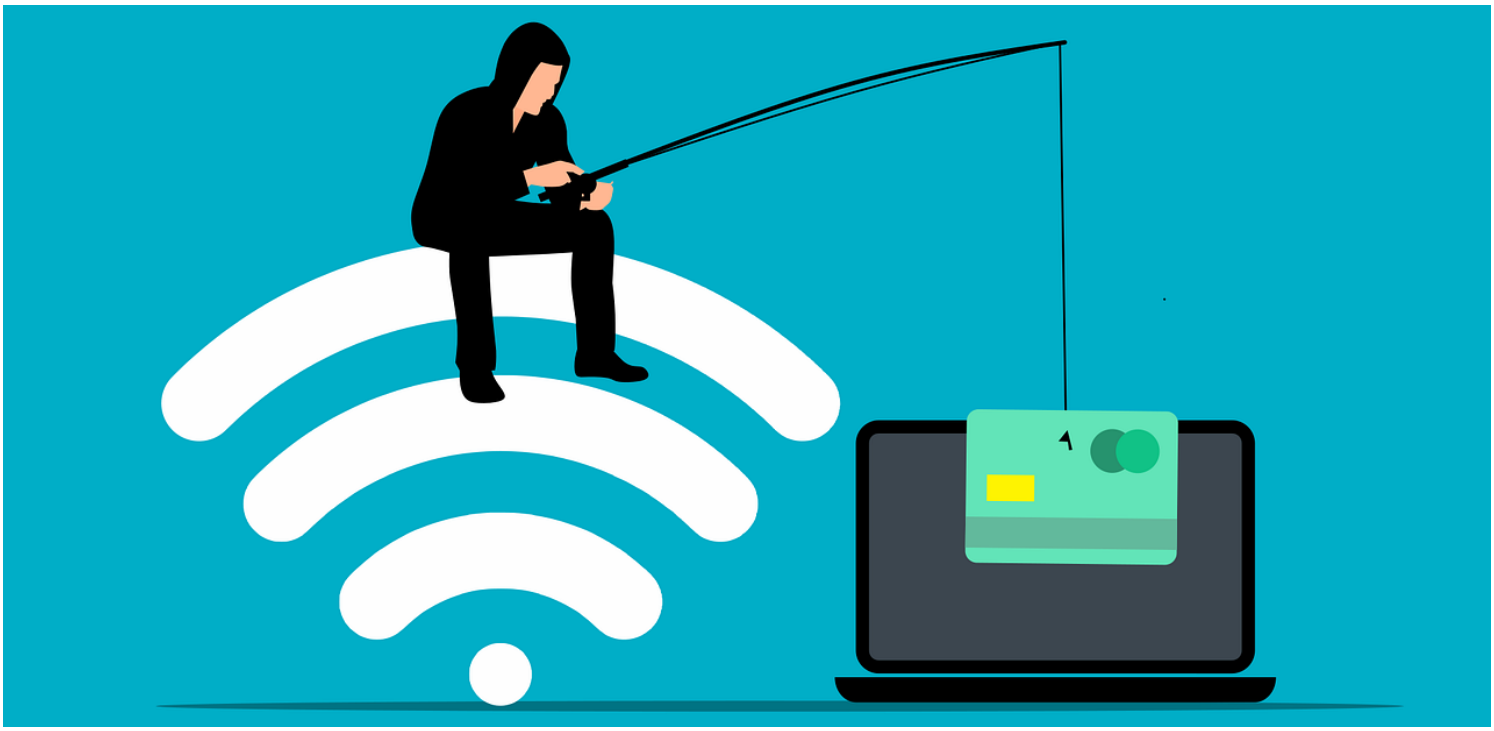
DAILY SCIENCE
DÉCOUVREZ LA SCIENCE, LA RECHERCHE ET L'INNOVATION "MADE IN BELGIUM"

LE PHISHING, PRINCIPALE PORTE D'ENTRÉE DES CYBERCRIMINELS

Publié le 25 octobre 2023



par Christian Du Brulle

Intelligence artificielle, industries culturelles et créatives, territoires connectés et intelligents: le numérique était à l'honneur au MTL connecte, le grand rendez-vous francophone des acteurs et des chercheurs actifs dans ce domaine. Une quatrième dimension y était également abordée: celle de la cybersécurité. Elle concerne tout le monde et est loin d'être négligeable!

« La cybersécurité? Cela englobe toutes les mesures raisonnables et acceptables destinées à protéger les technologies utilisées par les citoyens, les entreprises, les organisations et les autorités publiques contre les cybermenaces », rappelle Phédra Clouner, la Directrice générale adjointe du Centre pour la Cybersécurité Belgique, un centre qui dépend directement du Premier ministre. « La cybersécurité implique la protection des systèmes (tels que le matériel, les logiciels et l'infrastructure connexe), des réseaux et des données qu'ils contiennent », précise-t-elle.

Des attaques de diverses natures

« Et la menace ne fait qu'augmenter. Avec des impacts plus ou moins critiques selon les cibles visées », indiquait-elle à Montréal, où une délégation de 70 chercheurs et acteurs du numérique de Bruxelles et de Wallonie avait fait le déplacement, grâce à Wallonie-Bruxelles International et l'Awex.

Parmi les types d'attaques déployées par les cybercriminels, elle pointe l'accès illégal aux données et leur vol, les attaques de systèmes qui bloquent leur accès, quand les cybercriminels essaient de rendre un serveur indisponible en le surchargeant avec une très grande quantité de requêtes

(attaque par déni de service), la déviation du trafic vers de faux sites, le « rançongiciel », ou encore la diffusion d'informations protégées. « Les cybercriminels ne prennent même plus la peine de crypter vos informations sur vos serveurs, ils menacent désormais de les diffuser si vous ne payez pas », souligne-t-elle.

***Phishing*, *smishing*, *quishing*…**

Pour arriver à leurs fins, les cybercriminels utilisent toute une série de techniques, dont l'hameçonnage (*phishing*, en anglais). « Cette technique reste la méthode la plus fréquemment utilisée pour extorquer des identifiants, des données critiques, des mots de passe et ainsi avoir un accès aux données ou au réseau informatique de leurs victimes », souligne Mme Clouner.

Le *phishing* et ses diverses déclinaisons (*smishing* via sms par exemple, ou encore *quishing*, via le lien d'un QR code) tentent d'abuser la confiance de l'internaute par des faux messages invitant à cliquer sur des liens dirigeant vers de faux sites internet. Si le lien en question ne sert pas à installer un *malware* (un virus, un logiciel espion ou tout autre logiciel caché destiné ensuite à initier une cyberattaque ou à voler des données), la victime est amenée à indiquer ses mots de passe ou identifiants sur un site malicieux pour un service en ligne (mail, banque, commerce…).

Quasi 40 millions d'euros évaporés en 2022

« Les messages de *phishing* sont de plus en plus crédibles », rappelle-t-on au CCB, le Centre pour la Cybersécurité Belgique. « Ils ressemblent très fort à des messages réels. Nous remarquons que des messages de *phishing* consistent 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 un lien malicieux ou menant vers un faux site Internet. »

Les messages en question tentent de se faire passer pour des autorités (fédérales, régionales…), des fournisseurs d'énergie ou des sociétés de livraison. « Non seulement ces messages causent des nuisances, mais ils font aussi de nombreuses victimes. En 2022, 39,8 millions d'euros ont été dérobés en Belgique suite au *phishing* », souligne le Centre.

Une (bonne) adresse: safeonweb.be

Pour lutter contre ce phénomène, le CCB invite les destinataires de tels messages frauduleux à les lui envoyer via l'adresse « suspect@safeonweb.be ».

Safeonweb.be est le service d'information du CCB pour le grand public. On y retrouve toute une série de conseils et d'actualités en lien avec la cybersécurité en Belgique. Dont un nouvel outil pour lutter contre le *phishing*, lancé ce 16 octobre 2023 dans le cadre de la grande campagne de sensibilisation annuelle du CCB et qui a pour sujet… le *phishing*.

Il s'agit d'une extension pour navigateur web. Cet outil aide les citoyens à déterminer la fiabilité des sites web qu'ils visitent en attribuant un niveau de confiance (élevé, moyen, faible) à chaque site.

30.000 signalements par jour en Belgique

Pour avoir une idée de l'ampleur du phénomène de *phishing* en Belgique, les chiffres divulgués par Mme Clouner parlent d'eux-mêmes. « En 2022, suspect@safeonweb.be a reçu 5.973.239 mails de signalement de la part du public », souligne-t-elle.

« Depuis le début 2023, nous en recevons en moyenne 30.000 par jour ». Des signalements qui ne servent pas simplement à alimenter des statistiques (imparfaites puisque le signalement n'est pas obligatoire). Par contre, le CCB les passe à la moulinette pour identifier les sites d'envoi suspects.

« Nous traitons ces mails avec toute une série d'outils », détaille Phédra Clouner. « Cela nous permet d'identifier les domaines, les sites Internet malicieux qui sont à l'origine des campagnes de

DAILY SCIENCE
DÉCOUVREZ LA SCIENCE, LA RECHERCHE ET L'INNOVATION "MADE IN BELGIUM"

phishing (665.000 URL suspects ont ainsi été identifiés en 2022). Nous travaillons avec Microsoft et Google pour bloquer les sites malicieux. En parallèle, nous avons mis en place une page d'alerte, qui prévient l'internaute s'il tente d'accéder à un site Internet qui est considéré comme malicieux. En 2022, ce genre d'alerte (*warning page*) a été affiché plus de 14 millions de fois. »

« Plusieurs bonnes habitudes permettent de limiter fortement les risques », indique encore la Directrice générale adjointe du Centre pour la cybersécurité Belgique. « À commencer par la vérification de l'adresse qui expédie le message suspect. »

Le CCB propose sur Safeonweb une série de conseils judicieux à ce propos. Une adresse assurément non suspecte!