ORDRE DES MEDECINS
CONSEIL NATIONAL

ORDE DER ARTSEN
NATIONALE RAAD

Vigilance du médecin face à la cybercriminalité

Doc	a170006
Date de publication	25/02/2023
Origine	CN
Thèmes	Internet Informatique

Le Conseil national de l'Ordre des médecins a été récemment informé d'une nouvelle arnaque dirigée contre des médecins grâce à des informations recueillies sur Internet.

Un individu malveillant consulte les appréciations publiques mises sur la page Internet professionnelle d'un médecin afin d'identifier l'un ou l'autre de ses patients. Le médecin concerné est ensuite contacté téléphoniquement par une personne qui se présente comme un pharmacien à qui le patient, identifié sur la page professionnelle, aurait demandé la délivrance d'un médicament soumis à prescription (diazepam, zolpidem, etc.). Sous divers prétextes (pas de petit conditionnement, défaillance de la plate-forme eHealth, mauvais numéro NISS noté) le médecin est amené à prescrire un grand conditionnement du médicament et à communiquer oralement les codes des prescriptions et le numéro NISS du patient.

Comme l'illustre cet exemple, les médecins ne sont pas épargnés par la cyberfraude, dont les formes et les noms sont multiples (phishing, vishing, smishing, brandjacking, defacing, formjacking, angler phishing, spearphishing, spoofing, etc.).

La sécurité informatique doit être une préoccupation du médecin, tant sur le plan de la sécurité de l'outil informatique que sur le plan du bon comportement à adopter face aux risques et aux attaques.

Il est de son intérêt, mais aussi de celui des patients dont il traite des données, de veiller à se prémunir des actes de cybercriminalité.

Le respect des politiques de sécurité développées dans le milieu professionnel, notamment les institutions de soins, est essentiel.

Le Conseil national encourage les médecins à s'informer quant aux bonnes pratiques de prévention et à signaler les fraudes dont ils sont l'objet.

Le Centre pour la Cybersécurité Belgique (CCB) est l'autorité nationale en charge de la cybersécurité en Belgique (créé par l'arrêté royal du 10 octobre 2014). Son site fournit de nombreuses informations utiles, notamment sous forme de webinaires (https://ccb.belgium.be/fr/work).

A travers le site Safeonweb.be, le CCB informe les internautes au sujet de la sécurité en ligne et des mesures à adopter en cas de problème (https://www.safeonweb.be/index.php/fr/conseils; https://www.safeonweb.be/fr/au-secours).

Le site de la Cyber Emergency Response Team fédérale (CERT.be), service opérationnel du CCB, contient, outre des conseils, une page de signalement des incidents (https://cert.be/fr).

Le site de la police fédérale aborde également les questions relatives à la cyberprévention

https://www.police.be/5998/fr/questions/cyberprevention).

Ci-dessous, le rappel de quelques règles de base à adopter :

- vérifier la vulnérabilité de votre matériel informatique ;
- utilisez des mots de passe différents et robustes ;
- ne transmettez pas vos identifiants, mots de passe ou codes secret par téléphone ou e-mail ;
- considérez avec suspicion toute demande d'informations confidentielles et vérifiez que votre interlocuteur est légitime ;
- méfiez-vous des messages non sollicités, particulièrement s'ils ne sont pas personnalisés, s'ils requièrent une action urgente, s'ils visent à éveiller votre curiosité (« regardez ce que j'ai lu sur vous… ») ou adoptent un ton menaçant ;
- ne cliquez pas sur les liens contenus dans des messages non sollicités ;
- ne cliquez pas sur les liens et n'ouvrez pas une pièce jointe qui ne vous inspirent pas confiance
- considérez avec suspicion les messages officiels qui contiennent des fautes d'orthographe ou une formulation atypique (allez sur le site officiel pour contrôler l'information ou prendre contact);
- lisez attentivement l'adresse de l'expéditeur, les courriels frauduleux utilisent souvent une adresse qui ressemble à une adresse fiable avec une lettre interchangée ou un mauvais nom de domaine;
- considérez avec suspicion les offres « trop belles pour être vraies » ;
- soyez conscients que les réseaux sociaux permettent de recueillir des informations utiles pour personnaliser le phishing ;
- informez-vous régulièrement concernant la cybersécurité.

Remarque :

Le phishing consiste en un message reçu par email et envoyé à de nombreux comptes. L'objectif est que la cible télécharge ou ouvre un fichier, renseigne ses identifiants, ouvre une pièce jointe, dans le but d'amorcer une cyberattaque (fuite de données, ransomware, etc.). Cela peut se faire par e-mails mais également par SMS (smishing) ou messages sur les réseaux sociaux.

Le vishing est un type de phishing réalisé par le biais d'un appel téléphonique.

Le spearphishing est une version davantage ciblée et personnalisée du phishing. Le criminel identifie sa victime et recherche des informations personnelles la concernant pour créer un message d'apparence authentique et qui semble provenir d'une source de confiance.

Le angler phishing est un type de phishing qui vise les comptes de réseaux sociaux. Des hackers se font passer pour des agents du service client de ces réseaux (social phishing).

Le spoofing est une forme d'escroquerie dans laquelle les fraudeurs usurpent l'identité d'une autre personne pour mettre la cible en confiance. Ils se font passer pour un employé de banque, d'un service public ou d'une autre organisation connue.

Dans le brandjacking, l'arnaqueur se fait passer pour une entreprise connue, une grande marque ou une célébrité.

Le formjacking vise l'achat en ligne. Il a pour but de s'infiltrer dans le logiciel sous-jacent d'une

boutique en ligne, par exemple, pour y installer un logiciel malveillant.

En cas de defacing, le contenu des pages web est remplacé par un message ou un contenu activiste qui porte atteinte à l'image de l'entreprise. Les hackers empêchent l'accès au site web pour obtenir une rançon, tentent de voler des données sensibles, etc.