Attention : Le phishing de plus en plus présent

Plus de la moitié des Belges ont déjà été victimes de phishing en 2021 et le montant s'élève à environ 34 millions d'Euro.

Le phishing/hameçonnage est une méthode de vol qui consiste à envoyer de faux e-mail, de faux sms, à proposer des faux sites de vente ou bien encore passer des coups de téléphone au nom de différentes sociétés afin de dérober un somme d'argent à la victime. Le phishing touche tous les secteurs. Sur les 6 derniers mois, plus de 56% de la population belge a été victime d'hameçonnage/phishing. Febelfin met en garde et pousse les Belges à être plus vigilants lorsqu'ils reçoivent des e-mail,des sms ou des coups de téléphone suspects. (Romero, 2021)

Voici quelques exemples de nom d'entreprise qui ont été empruntés afin de tromper la population :

- *Bpost*
- *Les institutions bancaires telles que Belfius, ING, BNP, …*
- *Les SMS liés à la crise du coronavirus et du vaccin*
- *Les sociétés de télécommunication comme Proximus, VOO, orange, …*
- *Les institutions de l'état tels que le SPF finance*
- *Et bien d'autre encore …*

Depuis quelques jours, un nouveau logiciel malveillant circule par Windows 10. Il est appelé Bizarro, il vole les données bancaires des victimes. Il se propage par des envois de mails provenant soi-disant des institutions fiscales ou bancaires qui demande des informations personnelles afin de régulariser une situation urgente. Si la victime clique sur le lien fourni avec le mail, elle va permettre le téléchargement du logiciel qui va clôturer les sessions de la victime, un message d'une menace va s'afficher. Dès que la victime va relancer sa session, le logiciel va capturer les identifiants bancaires de la victime. Ses identifiants seront revendus sur le marché noir afin que le logiciel ne se rende pas coupable de vol bancaire. (info, 2021)

Pour éviter de se faire arnaquer, voici quelques petits conseils : *(Wattenbergh, 2021)*

- Ne jamais divulguer d'information personnelle ou bancaire par mail ou par sms ou même par téléphone.
- Ne jamais cliquer sur un lien douteux ;
- Vérifier l'adresse mail de l'expéditeur, vous pouvez le voir en faisant un clic droit avec votre souris sur le nom de l'expéditeur du mail. Le nom qui doit figurer après le @ doit être le nom de la société qui vous envoie cet e-mail ;
- Les fautes d'orthographe, de grammaire ou une mauvaise tournure de phrase peuvent être le signe d'un mail frauduleux ;
- La langue utilisée dans le mail ou le sms doit être votre langue maternelle ;
- Si le mail ou le sms comporte des menaces, il y a de grande chance pour que le mail ou le sms soit frauduleux. ;
- En cas de doute, aller voir sur internet s'il n'y a pas d'autres personnes qui ont reçu le même genre de mail ou de SMS ;
- La page Facebook Marnaque qui cite les arnaques fréquentes du moment ;
- …

Il existe des solutions si la victime est tombée dans le piège, comme :

- Faire opposition à sa carte bancaire ;
- Contester les opérations frauduleuses ;
- Déposer plainte auprès de la police ;
- Remplir le document de demande de remboursement auprès de la banque et joindre la copie du PV de police ;
- Porter plainte sur le site "www.pointdecontact.belgique.be"
- Garder les preuves (lorsqu'il y en a)