FICHE 9

PIGEON

Cette fiche renvoie à cet épisode du podcast

Toutes les ressources liées à la thématique sont disponibles dans ce tableau !

Internet, le royaume de l'escroquerie?

Dans la thématique sur la cybersécurité (fiche 6), nous vous parlions de piratage (appelé aussi hacking), cette manoeuvre au cours de laquelle un individu malveillant prend le contrôle d'un compte sur un réseau social, par exemple, dans le but de le détourner (dérober des données personnelles, professionnelles, bancaires, usurper l'identité, etc.). Des données sont donc manipulées à des fins malveillantes. Dans le cadre d'une arnaque, c'est bien souvent une personne qui est manipulée. Par exemple, quelqu'un peut abuser de votre confiance pour vous soutirer de l'argent. Tout autant punissable par la loi que le piratage, l'arnaque peut prendre de multiples formes.

C'est quoi le Phishing ?

Appelé également le hameçonnage, le phishing se présente le plus souvent via les mails indésirables, les spams mais aussi via des messages directs sur les réseaux sociaux ou sur votre téléphone. Bah oui, c'est bien pratique de savoir à quelle heure va passer le livreur Amazon. Mais du coup, la porosité entre un réel message d'organisation et des arnaques est de plus en plus grande. Concrètement, vous recevez d'une manière ou d'une autre une incitation à cliquer sur un lien, ouvrir un email, télécharger une appli sous un faux prétexte. Vos données sont alors «volées». Cela peut occasionner des dégâts importants comme une perte financière importante (en ayant accès à vos données bancaires) ou une usurpation d'identité (en ayant accès à vos dossiers personnels).

Il existe depuis peu une nouvelle invention : le quishing, contraction de QR code et phishing. C'est une technique pour voler de l'argent via de faux QR codes. Sachez que si vous êtes victimes de cette arnaque, votre banque peut vous rembourser si l'opération s'est faite automatiquement. En revanche, si vous avez encodé votre code, aucun remboursement n'est prévu.

Les influenceur.euses peuvent-ils arnaquer?

C'est quoi, un·e influenceur·euse? Il s'agit de personnes qui partagent des contenus via les réseaux sociaux sur des thématiques et leur mode de vie. Leur succès se mesure à la communauté qui les suit, le but étant qu'elle soit la plus nombreuse possible à

suivre régulièrement ce qu'iels postent. En toute logique, les marques ont vu dans ces influenceur·euses l'opportunité de faire de la publicité via des partenariats rémunérés, des collaborations ou des parrainages. C'est donc l'influence exercée par l'influenceur·euse sur sa communauté, grâce à sa popularité, sa proximité, son rôle de «modèle accessible», qui va avoir un impact sur la consommation des followers. Plus largement, on peut parler de marketing d'influence quand l'influenceur·euse reçoit une contrepartie financière ou en nature et que l'annonceur a son mot à dire sur la communication.

Quel cadre légal pour les contenus sponsorisés?

Un cadre a été imposé aux influenceur·euses à propos des contenus sponsorisés (c'est-à-dire quand iels reçoivent une contrepartie): la publicité doit toujours être identifiable comme telle et il en va de leur responsabilité de communiquer de manière claire et transparente qu'il s'agit d'un message commercial. L'expression «partenariat rémunéré» ou le hashtag «collab» ou «pub» sont des indices très clairs, par exemple.

Le problème, c'est que ces mentions sont écrites en minuscule sur des publications photo ou vidéo ou mentionnées en début de vidéo.

Le dropshipping

Il arrive régulièrement aux influenceur·euses de pratiquer le dropshipping, c'est-à-dire de proposer des produits en ligne sans en détenir les stocks. Ceux-ci sont chez un fournisseur qui peut se situer à l'étranger (un délai de livraison très long en est un indice). Et souvent, iels proposent des produits médiocres vendus 80 à 200 fois plus chers.

Aucune obligation légale n'impose au vendeur ou à la vendeuse de dire au client·e qu'iel pratique le dropshipping. Tout cela est donc légal mais source de nombreuses arnaques (colis défectueux, non-conformes, jamais envoyés, sans délai de rétractation...). La plus grande prudence est donc requise! On vous invite à regarder la vidéo d'Un Créatif à ce propos.

Et les autres types d'arnaques?

Il y a encore beaucoup à dire, malheureusement, sur les différents types d'arnaques qui existent en ligne et ailleurs... Nous ne pouvons que vous inciter à rester vigilant·es et à vous renseigner régulièrement à ce sujet. Sachez aussi qu'avec les progrès de l'intelligence artificielle, les arnaques peuvent prendre encore une autre dimension: qu'elle imite la voix, l'image ou le style d'écriture d'un·e de vos ami·es, elle a beaucoup de cartes en main pour vous duper. Mais n'oubliez pas non plus que des arnaques courantes existent aussi via SMS. De plus en plus de techniques commerciales se font via ce canal (La Poste, des entreprises de livraisons, Vinted, etc.) donc il est logique que des arnaques y fleurissent également, souvent en vous incitant à cliquer sur un lien.

A quoi être attentif·ve?

Pour éviter le piratage ou les arnaques, il n'y a pas de formule magique. Tout le monde est susceptible de se faire avoir. Nous ne sommes pas des pigeon·nes pour autant. Loin de là ! Les techniques se professionnalisent. A l'époque, de grosses fautes d'orthographe nous mettaient la puce à l'oreille. Aujourd'hui, déceler le vrai du faux devient très compliqué. Mais on peut limiter la casse.

Pour éviter de se faire pirater, déjà, on utilise des bons mots de passe (on vous renvoie vers la fiche 6 - Cyb3r $3cur1ty). N'oubliez pas non plus d'activer l'authentification à deux facteurs. En d'autres mots, pour vous connecter, on vous demande de confirmer votre identité via un autre canal. C'est loin d'être une perte de temps quand on sait le nombre de tentatives de piratage par jour.

Pour éviter les arnaques:

- on repère les comptes officiels des personnalités sur les réseaux sociaux. Par exemple, sur Instagram, il s'agit d'un badge V bleu à côté du nom de la personnalité. A présent payante, cette fonctionnalité "Méta verified" indique que la maison mère s'est assurée de l'identité de la personne concernée. De cette manière, vous pouvez davantage faire confiance à un compte officiel qui souhaiterait faire la promotion d'un produit. Même s'il est évident que nous vous conseillons de garder votre esprit critique en toute circonstance ;-)

- De manière générale, on suit son intuition et on fait appel à son bon sens. Ne cliquez pas sur un lien qui vous semble étrange, survolez-le avant d'éventuellement cliquer afin de voir vers quoi il renvoie, ne croyez pas que vous avez gagné un concours auquel vous n'avez pas participé, soyez très vigilants face à un mail qui vous demande de divulguer des données personnelles, vérifiez que votre connexion est sécurisée (avec le cadenas ou https dans l'url), utilisez des sites officiels pour les paiements.

Enfin, si on remarque des messages qui semblent suspects, on contacte suspect@safeonweb.be ou la ligne "pour un Internet plus sûr" de Child Focus, le 116000 (gratuit et accessible 24h/24)

E.R. : Ultra Vagues - www.ultravagues.com