FUTURA

Arnaques en ligne : tous les pièges et comment les éviter

Podcast écrit et lu par Emma Hollen

[*Générique d'intro, une musique énergique et vitaminée.*]

La saison des arnaques est ouverte, et c'est le décryptage de la semaine dans Vitamine Tech !

[*Fin du générique.*]

Si vous n'avez reçu aucun mail ou SMS suspect durant le printemps, vous demandant de vérifier votre déclaration d'impôts, ne baissez pas pour autant votre garde tout de suite. Car la rentrée marque l'ouverture de la saison des arnaques ! Fausses notifications de remboursement fiscal, amendes fictives prétendument collectées sur la route des vacances, sites offrant de découvrir dans quelle classe vos enfants vont se trouver : les arnaqueurs en ligne redoublent de créativité pour collecter alternativement votre argent ou vos données personnelles… et pourquoi pas les deux ! Bonjour à toutes et à tous, je suis Emma Hollen, en remplacement d'Adèle Ndjaki pour cette semaine du 2 septembre, et aujourd'hui, dans Vitamine Tech, on fait le tour des différents types d'arnaques en ligne et des astuces pour les déjouer.

[*Une musique électronique calme.*]

10 600 euros, 50 000 euros, 450 000 euros… Rien que cette année – et rien qu'en France – les récits d'arnaque les plus stupéfiants ont fait les gros titres à de nombreuses reprises. Et à chaque fois, c'est le même propos que tiennent les victimes : « Comment ai-je pu me faire avoir ? », « Je ne suis pourtant pas quelqu'un de naïf », ou encore « Même avec du recul, l'arnaque était impossible à déceler. » Il faut dire qu'il s'en est passé du temps depuis l'époque des premiers emails de phishing, tantôt bourrés de fautes d'orthographe, de récits d'héritage fantasques, ou de phrases tout en majuscules, en rouge, en gras, italiques et surlignées demandant de cliquer tout de suite sur un lien pour éviter de perdre le contenu de sa boîte mail. Aujourd'hui, les arnaqueurs virtuels disposent d'un vaste panel d'outils pour créer de faux sites toujours plus convaincants, envoyer des SMS portant le nom d'une agence gouvernementale comme expéditeur, ou encore rédiger des mails reprenant tous les codes des banques modernes. D'après Ani Petrosyan, chercheuse à l'université de Pennsylvanie, on estime à plus de 84 milliards d'euros le coût de la cybercriminalité subie par les internautes en France, en 2023. Et d'année en d'année, l'addition devient toujours plus salée.

Alors, sur quels supports peut-on s'attendre à trouver ces arnaqueurs invisibles ? Eh bien, c'est assez simple : si l'appareil que vous utilisez dispose d'une connexion, qu'elle soit téléphonique, WiFi, ADSL ou encore 4G, les risques d'arnaques ne sont jamais nuls. Du côté du téléphone, il est possible que vous receviez un appel concernant vos droits de formation via le fameux CPF, un message automatique vous réclamant le règlement par téléphone d'une facture, ou encore un coup de fil de votre banquier vous demandant de lui transmettre des informations urgemment afin de sécuriser votre compte. Dans tous ces cas, et dans bien d'autres, une alerte doit s'activer dans votre cerveau. Règle d'or numéro 1 : ne jamais transmettre de données bancaires ou personnelles via votre téléphone. Numéro de carte bleue, de sécurité sociale, même adresse personnelle ou créneaux d'absence de votre domicile : si vous n'êtes pas absolument certain ou certaine de reconnaître personnellement votre interlocuteur, et de le juger de confiance, ne communiquez aucun de ces éléments. Et même si vous reconnaissez sa voix, sachez qu'aujourd'hui, l'intelligence artificielle, et plus particulièrement les deepfakes permettent d'imiter le timbre d'une personne à partir de seulement quelques secondes d'enregistrement. Aujourd'hui, cette technique sert non seulement à soutirer des informations, mais également à faire croire à des kidnappings, permettant d'extorquer des rançons aux montants considérables. Soyez donc vigilants et restez attentifs à tout comportement ou question qui vous semblerait anormal ou improbable. Bien souvent, les arnaqueurs vous ferons croire à une situation urgente pour vous obliger à agir rapidement et sans réfléchir. Dans ce cas, la meilleure option est de raccrocher ou de mettre en attente l'appel et de contacter vous-mêmes le numéro de l'interlocuteur que vous êtes censé·e·s avoir au téléphone. C'est ainsi par exemple qu'une mère américaine a échappé à une fausse demande de rançon, en ayant la présence d'esprit d'appeler le portable de sa fille prétendument enlevée. Cette dernière, dont elle entendait pourtant la voix paniquée au bout du fil de l'arnaqueur, lui a répondu sur son propre téléphone en lui assurant que tout allait bien. Dernier point de méfiance : le ping call, une pratique consistant à appeler très brièvement une personne puis à raccrocher. Bien trop souvent, la victime, voyant un appel manqué, rappellera le numéro qui s'avère fortement surtaxé. De façon générale, pour éviter les problèmes, vous pouvez vous rendre sur le site bloctel.gouv.fr, qui vous permettra, d'une, de signaler les numéros douteux et, de deux, de vous protéger – dans une certaine mesure – contre le démarchage abusif.

Alors, ne faut-il plus se fier qu'à ses yeux, s'ils fonctionnent ? Eh bien, à l'ère de l'intelligence artificielle, il ne suffit plus de voir pour croire. Une fois encore, ce sont les deepfakes qui permettent de reproduire l'apparence d'une personne de manière de plus en plus convaincante, et ce, en temps réel ! C'est ainsi qu'en février, un employé d'une firme internationale a viré plus de 23 millions d'euros à un groupe d'arnaqueurs, qui ont réussi à se faire passer pour ses collègues ainsi qu'un directeur financier lors d'une visioconférence. Les deepfakes sont également de plus en plus souvent employés lors d'escroqueries à l'escorte, d'arnaques sentimentales ou de chantages sexuels. Derrière la personne séduisante qui apparaît à l'écran se cache un opérateur qui tentera d'obtenir de l'argent soit via de fausses transactions, via du chantage affectif ou encore, en obtenant des images compromettantes de la victime, qu'il menacera de faire circuler sauf versement d'une rançon. Une fois encore, la vigilance est de mise, en particulier avec les personnes que l'on connaît uniquement via internet. Même pour un entretien d'embauche en ligne, attention à ne fournir aucune information sensible sans vous être amplement assuré·e du niveau de sécurité de votre échange. Et dans le cas de personnes que vous connaîtriez par ailleurs, une double vérification est toujours utile avant de faire circuler des infos ou des fichiers susceptibles d'être utilisés contre vous. Gardez en tête qu'un compte peut toujours être

piraté et que l'utilisation du bon profil ou de la bonne adresse email ne sont jamais une garantie d'authenticité. Notez enfin que la même vigilance s'impose dans le cas des messageries instantanées : Messenger, WhatsApp, Teams, Telegram, etc.

[*Virgule sonore, une cassette que l'on accélère puis rembobine.*]
[*Une musique de hip-hop expérimental calme.*]

Si l'on se tourne désormais du côté des SMS, plusieurs cas de figure peuvent, là également, se présenter : on vous pourra vous demander de répondre au texto, chaque SMS que vous envoyez étant généralement surtaxé, on vous encouragera à rappeler un numéro, lui aussi surtaxé, pour consulter votre messagerie par exemple, ou encore on vous proposera de cliquer sur un lien vers un site où vous pourrez soi-disant consulter votre CPF ou régler une amende. Dans ce dernier cas, la meilleure option consistera à tout simplement à chercher directement l'adresse du service concerné sur internet. Par exemple, si Enedis vous envoie un lien par SMS en vous demandant de renseigner vos consommations, comme cela peut arriver chez les particuliers n'ayant pas de compteur communiquant, vous pouvez certes cliquer sur le lien et vous assurer qu'il vous mène sur une URL valide, à savoir enedis.fr, mais le mieux est encore de chercher Enedis sur votre moteur de recherche préféré et de vous rendre directement sur leur site, où vous pourrez vous connecter puis renseigner les informations demandées. Je précise que cet épisode n'est pas sponsorisé par Enedis.
Et puisqu'on parle de bonnes pratiques en matière de liens, il en va de même pour les emails. De nos jours, un email peut reprendre l'apparence exacte d'un message envoyé par votre banque, et vous proposer de cliquer sur un bouton pour consulter vos comptes ou fournir un nouveau mot de passe. Là encore, la prudence est de mise, et mieux vaut passer par votre moteur de recherche ou bien par vos liens enregistrés en favori, pour vous rendre sur le site de votre banque, de votre assureur, des impôts ou encore de votre mutuelle. Vraiment, méfiez-vous. Il y a quelques années, j'ai ouvert par curiosité l'un de ces emails, venu d'une banque à laquelle je n'étais pas cliente. J'ai cliqué sur le bouton censé me mener sur mon compte personnel et me suis retrouvée sur un site d'une vraisemblance confondante. L'interface semblait authentique, l'URL semblait correcte au premier coup d'œil, et même un clic sur le logo de la banque en haut de page me ramenait sur sa page d'accueil. C'est uniquement parce que je savais avoir affaire à une arnaque que j'ai fini par déceler un court préfixe au début de l'URL m'indiquant que j'étais sur un site contrefait. Une fois de plus, on redouble donc de vigilance ! Toujours dans la catégorie des emails, attention aux pièces jointes que vous téléchargez, méfiez-vous bien évidemment des messages d'inconnus tentant d'établir des relations personnelles ou vous demandant des faveurs – attention aussi aux mails d'employeurs potentiels, de notaires ou de services médicaux vous réclamant des informations sensibles – et enfin, méfiance même contre les messages d'amis, dont la messagerie peut avoir été piratée. Ainsi, il n'est pas impossible de recevoir un mail directement depuis l'adresse authentique de votre proche, vous demandant de le dépanner d'une certaine somme d'argent, pour une opération chirurgicale ou un billet d'avion par exemple. Dans ce cas, appelez votre proche ou contactez-le via un autre canal que l'email pour vous assurer que la demande est légitime, ce genre de message étant tout de même hautement improbable dans la plupart des cas. Si votre proche vous dit que le message ne venait pas de lui, pensez bien à lui recommander de changer le mot de passe de sa boîte mail, voire de consulter un spécialiste pour s'assurer que celle-ci est à nouveau protégée.

On poursuit avec les sites. Vous vous dites peut-être qu'on a déjà bien fait le tour avec les mails et les SMS, mais notez qu'un site n'a pas forcément besoin d'être relayé par message direct pour être dangereux. On peut retrouver des liens douteux sur les forums, dans les commentaires ou les posts sur les réseaux sociaux, mais aussi, tout simplement, via une simple recherche en ligne. Que vous soyez malade et cherchiez un traitement, que vous désiriez vous former, acheter un kit d'effets visuels, soutenir une cause, comparer des assurances ou gagner de l'argent rapidement, il y aura forcément un piège répondant à ces besoins, ou plutôt des centaines de pièges, tendus quelque part sur le web. Bon, ce n'est pas une raison pour devenir parano dès aujourd'hui, mais un peu de bon sens s'impose tout de même. Si vous utilisez un site pour la première fois, n'hésitez pas à vérifier sa réputation en ligne avant d'y acheter ou télécharger quoi que ce soit. N'acceptez jamais un téléchargement sans faire preuve d'une grande précaution, qu'il s'agisse d'un logiciel ou de tout autre produit ou fichier dématérialisé. Assurez-vous de l'origine de son auteur, qu'il correspond bien au type de fichier que vous souhaitiez télécharger en vérifiant son suffixe, et idéalement, passez-le au crible d'un logiciel anti-malware. Enfin, redoublez de vigilance sur les sites qui vous proposent une gratification importante et rapide contre un investissement : sites pornographiques, de jeu en ligne ou encore prétendus services destinés à faire fructifier votre argent. Dans ce dernier cas, de nombreux services proposent désormais de toucher un salaire de rentier voire de devenir millionnaire avec un minimum d'effort, grâce à des organisations pyramidales, de prétendues astuces, ou plus récemment, grâce à l'intelligence artificielle, qui pourrait soi-disant gérer vos actions pour vous. Je vous en parle plus en détails dans l'épisode de Vitamine Tech baptisé : « Arnaque sur les réseaux : « gagnez de l'argent rapidement grâce à cette astuce »… ou pas. » Avant de faire chauffer la carte bleue, prenez le temps de la réflexion et dans le cas d'opérations financières, faites-vous conseiller par un expert, banquier ou conseiller indépendant. Toute opération financière miracle demandant l'investissement d'un capital de départ doit faire retentir une sonnette d'alarme et vous appeler à faire preuve de discernement. On pense toujours être plus malin que les autres, jusqu'au moment où on se fait avoir. Si vous vous sentez dépassés par une addiction aux jeux en ligne ou à la pornographie, des professionnels de santé sont à votre disposition.

Dernier petit point et promis, c'est fini, même les appareils électroniques non connectés peuvent présenter un risque : bien évidemment, si vous trouvez une clé USB ou un disque dur abandonnés, n'essayez surtout pas de les brancher sur votre ordinateur !

Quelques bonnes pratiques pour terminer : utilisez des mots de passe différents sur chacun des sites que vous visitez. Vous pouvez les rassembler en un seul outil qui se chargera de les remplir pour vous, soit via le gestionnaire de mot de passe de votre navigateur, soit via un service dédié. Et bien évidemment, choisissez un mot de passe efficace pour sécuriser le coffre-fort contenant… tous vos autres mots de passe. Tenez-vous informé·e des dernières actualités concernant le phishing ou plus généralement les arnaques : connaître les coulisses d'une escroquerie permet de réduire considérablement son efficacité. Si vous vous sentez dépassé·e par les technologies mais en avez besoin régulièrement pour échanger des messages ou y déposer des informations confidentielles, demandez de l'aide à votre entourage, voire, suivez une formation, en ligne ou en présentiel, pour mieux vous familiariser avec ces nouvelles interfaces. Je vous joins en description un lien vers francenum.gouv.fr qui liste plusieurs formations gratuites pour se perfectionner sur les outils du numériques. Pour finir, si vous avez été victime d'une arnaque – et cela peut arriver à tout le monde – vous pouvez déposer une plainte via le téléservice THESEE ou bien contacter la ligne verte Info-Escroqueries au 0 805 805 817. Et enfin, restez alertes, tout

simplement. Contre les arnaques, en ligne, comme ailleurs, du bon sens et une bonne dose de prudence sont vos meilleurs alliés.

[*Virgule sonore, un grésillement électronique*.]

C'est tout pour cet épisode de Vitamine Tech. Pour ne pas manquer nos futurs épisodes, abonnez-vous dès à présent à ce podcast, et si vous le pouvez, laissez-nous une note et un commentaire. Cette semaine, je vous invite à découvrir notre dernier épisode de Science ou Fiction dans lequel Melissa Lepoureau vous dira si le mode nuit des écrans aide vraiment à mieux dormir. Pour le reste, je vous souhaite une excellente journée ou une très bonne soirée et je vous dis à la prochaine dans Vitamine Tech.

[*Un glitch électronique ferme l'épisode*.]