FUTURA

Arnaque sur les réseaux : « gagnez de l’argent rapidement grâce à cette astuce »… ou pas

Podcast écrit et lu par Emma Hollen

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

Des astuces pour gagner de l’argent rapidement sur Internet, c’est l’actu de la semaine dans Vitamine Tech.

[*Fin du générique.*]

[*Plusieurs voix de jeunes hommes se font suite, séparées les unes des autres par un bruit de statique, comme si l’on changeait de chaîne.*] « *Bonjour et bienvenue dans cette vidéo, dans laquelle nous allons découvrir cinquante façons de gagner de l’argent sans travailler.* » « *Wooow ! Attendez ! Ceci pourrait vous rendre riche !* » « *Ouais, t’as bien lu. Là j’te montre comment faire 15 euros avec ton téléphone et ça, dès maintenant.* » « *Dans les prochaines minutes, tu vas découvrir trois méthodes pour gagner de l’argent avec [*nom bippé*], qui est le leader mondial de la cryptomonnaie.* »

[*L’animatrice reprend la parole.*] Vous l’avez compris, aujourd’hui, on va parler des arnaques qui vous promettent de gagner de l’argent rapidement sur les réseaux sociaux. Un secteur florissant d’Internet qui, même s’il a connu un léger déclin en 2022, continue de se renouveler et de faire de nouvelles victimes.

[*Une musique électronique calme.*]

Le 24 mars dernier, la célèbre chaîne YouTube Linus Tech Tips a été victime d’une attaque un peu particulière. Aux alentours de 3 heures du matin, la chaîne aux 15,3 millions d’abonnés a subitement été renommée en *Tesla* et a démarré la diffusion live d’un podcast vidéo présentant Elon Musk en grande discussion avec plusieurs invités. Pas de *deepfake* ici, rien qui ne semble alarmant dans la vidéo elle-même, si ce n’est que, d’une : ces changements avaient lieu alors que le créateur de la chaîne dormait profondément ; de deux : ce contenu n’avait rien à voir avec les productions habituelles de la chaîne ; de trois : la vidéo était en fait un ancien podcast se faisant passer pour une diffusion live aux audiences boostées par des bots ; et pour finir : la description du stream invitait les utilisateurs à se rendre sur un site en leur promettant que pour chaque Bitcoin qu’ils y investiraient, Elon Musk leur en renverrait le double. Normalement, une alarme devrait s’être engagée dans la tête de tout·e internaute habitué à repérer les arnaques. Le site, d’apparence professionnelle, accueille les visiteurs avec une photo d’Elon Musk et l’annonce que ce dernier a lancé une opération spéciale pour booster l’expansion du Bitcoin. « *Nous croyons*

que la crypto et le Bitcoin vont changer le monde », déclare le site. « *Pour accélérer l'adoption en masse de la cryptomonnaie, nous avons décidé d'organiser la distribution de 1 000 Bitcoin aux détenteurs de crypto.* » Plus loin sur le site, une liste de fausses transactions s'actualise régulièrement, montrant combien d'argent des utilisateurs fictifs ont remporté grâce à cette opération. Tout est fait pour instiller dans l'esprit des utilisateurs un sentiment d'urgence et les pousser à sortir la carte bleue au plus vite : depuis la mention d'une opération limitée dans le temps mais dont les dates ne sont pas fournies, à la cagnotte de 1 000 Bitcoin que les investisseurs devront se partager, en passant par la liste des investissements qui s'actualise sous vos yeux en vous laissant comprendre qu'il n'y a pas de temps à perdre si vous voulez vous aussi récupérer votre part du gâteau. Nul besoin de dire qu'une fois votre virement vers le site réalisé, vous ne verrez plus jamais la couleur de vos précieux Bitcoin. La chaîne principale de Linus Tech Tips ainsi que deux autres chaînes secondaires, également hackées, ont finalement été suspendues par Youtube au bout de quelques heures et ce n'est que plus tard dans la journée que le créateur est parvenu à les récupérer dans leur état d'origine. Dans une vidéo postée peu de temps après l'attaque, Linus Sebastian raconte ses déboires et révèle notamment l'astuce, somme toute simple mais redoutablement efficace, employée par les hackers pour prendre le contrôle de son compte. Un des employés de son équipe aurait reçu une proposition commerciale par mail avec un document en pièce jointe fournissant les détails de l'offre. Si rien ne semblait alarmant de prime abord, il s'est avéré *a posteriori* que la pièce jointe en question contenait un malware, possiblement le fréquemment utilisé RedLine Stealer, qui s'est installé sur l'ordinateur de l'utilisateur au moment de l'ouverture du document. Ce malware a pour rôle de voler toutes sortes de données stockées sur votre navigateur, et notamment les cookies de session. Lorsque vous fermez Messenger, Gmail ou Instagram sur votre navigateur et les rouvrez quelques temps plus tard, vous n'avez normalement pas besoin de vous reconnecter. Pour cela, vous avez à remercier votre cookie de session, un petit fichier qui vous évite d'avoir à vous identifier à chaque fois que vous revenez sur un site. C'est très pratique pour vous, mais également pour le pirate qui, une fois muni de ce cookie, peut tranquillement accéder à votre chaîne YouTube et modifier ses paramètres, comme son nom et sa photo, ou encore y uploader des vidéos, le tout sans avoir besoin de votre mot de passe ni du code d'authentification à deux facteurs. C'est exactement ce qu'il s'est passé avec Linus Tech Tips, mais également avec de nombreuses autres chaînes Youtube qui ont été récemment visées par l'attaque. Car « l'arnaque au Musk », si on peut l'appeler ainsi, n'est pas un cas isolé ni même un cas récent. En juin 2022, un article de la BBC faisait déjà état d'occurrences similaires en cours depuis plusieurs mois, avec des attaques tout aussi bien sur la chaîne de l'armée britannique que sur le compte Vevo de Taylor Swift ou de Drake. Pour autant, YouTube ne semble pas pressé de mettre en place des mesures solides pour endiguer le phénomène, à la grande frustration des créateurs et de leur public. Et malheureusement, la plateforme est loin d'être le seul réseau social à voir fleurir les arnaques à l'investissement.

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

Une étude de l'AMF, l'Autorité des Marchés Financiers, menée en décembre 2021, révèle que la pandémie de Covid-19 a été particulièrement propice à l'explosion d'un florilège d'arnaques en 2020. Nous avons tous et toutes reçu ces SMS et ces mails de phishing nous invitant à nous rendre sur notre compte CPF pour débloquer des crédits, ou à entrer nos

données de sécurité sociale sur des sites obscurs. Mais une autre portion des fraudeurs a pour sa part investi les réseaux sociaux, comme TikTok, Facebook, Instagram, WhatsApp, Snapchat ou encore YouTube, pour ne citer que les principaux. Les maigres rendements des produits d'investissements, les confinements successifs, amenant les Français à passer plus de temps seuls en ligne et à moins dépenser, ou encore l'explosion du Bitcoin fin 2020 ont été autant de facteurs propices à l'apparition de toutes sortes d'arnaques, prêtes à capitaliser sur votre envie de trouver l'âme sœur, votre besoin de compléter vos revenus, ou votre ambition de devenir le nouveau roi de la crypto. Une étude de la Commission fédérale du commerce aux États-Unis, la FCC, rapporte qu'en 2021, 95 000 victimes auraient perdu un total de 770 millions de dollars sur les réseaux sociaux seuls. Et comme le souligne judicieusement leur communiqué, ce chiffre n'est que la partie émergée de l'iceberg, celle composée des personnes qui auront signalé leurs pertes. Les arnaques à l'investissement en particulier semblent connaître un véritable succès sur ces plateformes, en vous proposant alternativement d'acheter de la cryptomonnaie, de monter votre propre arnaque grâce à une formation coûteuse, ou de générer des revenus passifs à l'aide d'un service en ligne qui vous indiquera, contre un abonnement, dans quelles actions placer votre argent. [*De nouveaux extraits ponctués de statique.*] « *Dans cette vidéo, on va aborder en détail comment maximiser sa rentabilité afin de gagner gros sur le long terme.* » « *Gagne 10 euros à chaque fois que tu regardes une vidéo sur Youtube.* » « *Cette application m'a rapporté 2 000 euros pour le mois de juillet.* » « *Le job étudiant le mieux payé. Rejoins le club des gagnants en trouvant le meilleur emploi pour toi dès maintenant.* » [*L'animatrice reprend.*] Ça vous semble tentant ? Vous pensez savoir distinguer une vraie opportunité d'une arnaque ? C'était probablement aussi le cas des 26 170 Britanniques qui ont déclaré avoir collectivement perdu plus de 890 millions de livres en 2021 dans ce type d'affaires. Malheureusement, il n'existe pas de solution miracle pour gagner de l'argent rapidement, en quantité et sans travailler. À moins peut-être d'être déjà très riche et de posséder une éducation financière approfondie, comme le souligne avec amertume la journaliste Liz Aldrich pour le site *Money Made*. Derrière le ton intimiste de ces influenceurs, leurs titres accrocheurs et leurs vidéos alléchantes de promenades en Lamborghini et de cocktails sur la plage ne se cachent rien de plus que de belles paroles qui leur rapporteront gros… et ne vous apporteront rien. Alors, la prochaine fois que vous serez sur TikTok ou Facebook, rappelez-vous simplement de cette phrase : si ça semble trop beau pour être vrai, c'est que ça l'est probablement.

[*Virgule sonore, un grésillement électronique.*]

C'est tout pour cet épisode de Vitamine Tech. Si ce podcast vous plaît, pensez à vous abonner, et si vous le pouvez, laissez-nous une note et un commentaire pour nous dire ce que vous en avez pensé. Cette semaine, je vous invite à découvrir notre dernier épisode de Bêtes de Science, qui a, j'ai le grand plaisir de vous l'annoncer, repris du service. Vous y retrouverez Agatha Liévin-Bazin pour un voyage au Cameroun, sur les traces de l'étonnant gris du Gabon. Sur ce, je vous souhaite une excellente journée ou une très bonne soirée, et je vous dis à la semaine prochaine, dans Vitamine Tech.

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