Failles Sécu

Transcription

Épisode 12 : Mon ordi télétravaille tout seul, une aubaine ?

Speaker1 : Bonjour à tous et à toutes et bienvenue dans Failles Sécu, épisode 12 du 05 Novembre 2024 intitulé, « Mon ordi télétravaille tout seul, une aubaine ? » .

Speaker2 : Vous travaillez à distance pour une grande entreprise et on vous propose de travailler pour vous à distance ?

Speaker1 : Qui se cache derrière ces proposition ? On va le découvrir dans ce nouvel épisode de Failles Sécu!

##Jingle Début##

Speaker1 : Alors je suis Léa l'animatrice de cette émission qu'on essaie de garder mensuelle et voici notre spécialiste de l'informatique, mon cher ami Charlie! Toujours en vadrouilles ?

Speaker2 : Salut Léa, heureux de te retrouver pour notre douzième épisode, et bonjour à tous nos auditeurs et auditrices fidèles. Pour répondre à ta question, oui je suis encore en vadrouilles ce mois-ci, du côté de Narbonne plage, dans le département de l'Aude.

Speaker1 : Super, tu auras plus de chance de voir le soleil qu'ici à Paris! Alors de quoi va-t-il être question dans cet épisode ? Car le titre est assez énigmatique!

Speaker2 : On va parler de propositions que reçoivent certains développeurs en télétravail. On leur propose de travailler pour eux. Les conséquences de ces arnaques peuvent être dramatiques tant pour l'employé que pour l'entreprise. C'est pourquoi il m'a semblé important d'informer nos auditeurs sur ce sujet.

Speaker1 : Avant qu'on commence, si ça ne te dérange pas, je voudrais te parler d'un problème qui me met mal à l'aise.

Speaker2 : Vas-y allonge toi, tu peux tout me dire! Attends, je vais te mettre une musique relaxante pour te détendre.

Speaker2 : Ah, voilà!

##Musique de Relaxation##

Speaker1 : Te fiche pas de moi, c'est pas drôle.

Speaker2 : Aller, vas-y, vide ton sac!

Speaker1 : Voilà, ça fait quelques semaines que je suis harcelé par quelqu'un qui dit m'avoir observé. Il dit qu'il sait ce que je fais sur mon ordi et peut le révéler à tous mes contacts.

Speaker2 : Mais ça c'est une arnaque, on en reçoit tous les jours de tels messages!

Speaker1 : Oui je sais, d'habitude je n'y prête pas attention, mais là ça a l'air sérieux. Je me demande comment cette personne qui me harcèle peut savoir tout ça sur moi.

Speaker2 : Tu peux être plus précise, qu'est-ce qu'elle sait exactement sur toi ?

Speaker1 : Et bien son message commence par "Bonjour Léa", suivi de mon vrai nom de famille alors que je ça ne figure pas dans mon adresse électronique. Ensuite mon harceleur utilise une image de mon immeuble, ma date de naissance et mon numéro de téléphone perso que je ne communique qu'à mes proches. Et ils me réclament zéro virgule un bitcoin pour ne pas révéler l'affaire à mes contacts. Alors je m'en fiche qu'ils révèlent ce que je fais sur mon ordi à mes contacts, je ne fais rien d'illégal. Non, ce qui me tracasse c'est qu'ils aient accès à mes données personnelles. Alors voilà, j'aimerais que tu m'expliques comment ils font pour en savoir autant sur moi.

Speaker2 : OK, bon c'est bien une arnaque, et de nombreuses personnes reçoivent ce même type de menace, avec demande de rançon. Tu as dû passer à côté d'un email de ton opérateur téléphonique, ou de tel ou tel marchand qui t'informait d'une fuite de données personnelles suite au piratage de leur infrastructure informatique.

Speaker1 : Ah oui, probablement, j'ai un filtre de messagerie qui envoie tout ça directement à la poubelle!

Speaker2 : Alors je te fais un rappel. Tous les jours, des entreprises se font pirater et aspirer leur base de données clients. C'est ce qu'on appelle une fuite de données personnelles. Rien que cette année, ça a eu lieu chez SFR, chez Free, chez Picard, ou même chez France Travail. Ça fait donc beaucoup de données personnelles qui ont fuité. Pour être plus clair, ça veut dire qu'à peu près tout le monde a ses données personnelles qui circulent.

Speaker1 : Mais comment ça se fait que les entreprises arrivent à se faire voler leur base de données clients ? Elles ne prennent pas aux sérieux la protection des données de leurs clients ?

Speaker2 : Vaste question! Mais pour rester bref et technique, voici une illustration qui va permettre à nos auditeurs de comprendre. Imagine la sécurité informatique d'une entreprise comme une chaîne qui empêche l'entrée aux personnes non autorisées. Cette chaîne de sécurité est constituée de maillons qui représentent tous les éléments réels en lien avec la sécurité de l'entreprise. Et bien, comme dans une vraie chaîne, la robustesse de cette chaîne de sécurité dépend de son maillon faible.

Speaker1 : Quand tu parles d'éléments en lien avec la sécurité, tu veux dire les pare-feux, les anti-virus, les logiciels qui scrutent le trafic pour repérer des motifs d'attaquant,

Speaker2 : Oui mais pas seulement! Tu as aussi le personnel qui travaille dans cette entreprise, et qui peuvent visiter des sites dangereux, ou cliquer sur des liens piégés.

Speaker1 : Ah oui, tu veux dire que ces personnes peuvent faire entrer des virus et infecter ensuite tout le réseau de l'entreprise, alors que l'entreprise est super bien protégée ?

Speaker2 : Exactement! Mais ça peut aussi être des mot-de-passes utilisateur trop simples, ou encore des failles de sécurité dans des logiciels installés.

Speaker1 : Attends, tu veux dire que si j'installe un logiciel sur mon ordi d'entreprise et que ce logiciel comporte une faille de sécurité, je peux mettre en danger toute la sécurité de l'entreprise ?

Speaker2 : Oui c'est tout-à-fait possible si cette faille vient à être exploitée seule, ou combinée à une autre faille dans un autre logiciel utilisé dans l'entreprise.

Speaker1 : Et si j'ai installé des applis pourries sur mon téléphone et qu'ensuite je le connecte au réseau de l'entreprise, je mets aussi en péril la sécurité de l'entreprise ?

Speaker2 : Oui c'est bien probable! Et tu peux aussi ajouter que si ton entreprise super hyper sécurisée fait appel à un sous-traitant mal sécurisé pour réaliser une tache quelconque avec accès au réseau interne de ton entreprise. Et bien tu mets aussi en péril la sécurité de ton entreprise. Pareil si un employé clique sur un lien qui l'amène vers un faux site et entre son vrai mot-de-passe.

Speaker1 : C'est vertigineux, ça ne s'arrête jamais ?

Speaker2 : C'est bien tout l'objet de la sécurité informatique. Limiter au maximum la surface d'attaque de l'entreprise afin d'éviter que des intrus puissent s'infiltrer dans ton entreprise. C'est plus facile de protéger un petit abri au milieu de la forêt qu'un énorme hangar en plein désert!

Speaker1 : Ok je comprends. Donc là tu as répondu à la partie de ma question sur comment les entreprises parviennent à se faire pirater. Mais pourquoi en premier lieu des intrus ou voleurs veulent-ils dérober ces bases de données clients à une entreprise ?

Speaker2 : Et bien tout simplement car des personnes malveillantes sont prêtes à payer pour obtenir des informations d'entreprises cibles. Pense aux espions de pays étrangers par exemple. Et pas-à-pas elles se rapprochent de leur cible. Et le Graal, c'est la réutilisation de mot de passe.

Speaker1 : Attends tu veux dire que les pirates s'en foutent royalement de la base de données Picard, et que untel achète toutes les semaines les tagliatelles à la sauce merlu à 3€40 ? Mais si ce untel a utilisé chez Picard le même mot-de-passe que dans son entreprise super hyper protégée, alors les pirates peuvent tranquillement entrer dans le système informatique de l'entreprise et consulter les documents internes confidentiels ou secrets, simplement grâce au mot-de-passe glané chez Picard ?

Speaker2 : Oui ça peut-être une sorte d'utilisation de base de données clients.

Speaker1 : Et c'est pour ça que ça se vend sur l'internet caché alias le dark web!

Speaker2 : Exactement, et c'est pour ça que des pirates passent leur temps à tenter de pirater n'importe quel site.

Speaker1 : Car il y a de l'argent illégal à se faire! En tant qu'individu, on peut faire quelque chose contre ça ?

Speaker2 : Bien sûr, en tant que client tu n'as pas la main sur le niveau de sécurité informatique du magasin du coin qui te propose un compte client. Mais tu peux toujours utiliser un mot de passe différent pour chaque site. Firefox propose par exemple de te générer un mot de passe sécurisé, et de le retenir pour toi. C'est la, chose à faire. Ne jamais réutiliser les même mots de passe. Et si possible utiliser des alias de messagerie, comme propose Firefox relay.

Speaker1 : On dirait que tu travailles pour Firefox! Tu ne cites qu'eux!

Speaker2 : Oui c'est vrai, il existe d'autres solutions, mais je ne les connais pas et Firefox est gratuit et sécurisé. C'est pour ça que je me permets de les citer. Mais ils ne soutiennent pas cette émission.

Speaker1 : OK, je te laisse reprendre sur les actions que les clients peuvent prendre pour éviter que leurs données personnelles se retrouvent dans la nature.

Speaker2 : Donc en premier, on utilise des mots de passe complexes, et différents pour chaque site, sans jamais réutiliser le même, même s'il est très complexe. Car s'il est compromis sur un site, les pirates vont l'essayer sur d'autres sites. Mon deuxième conseil consiste à mentir sur votre adresse, votre date de naissance, ou tout autre donnée personnelle.

Speaker1 : Mentir à Picard c'est facile, mais à France Travail, c'est plus difficile et il me semble que c'est illégal en prime.

Speaker2 : Tu as raison. En règle générale, pour tout ce qui est banque, assurance, impôts, employeur, tu ne peux pas facilement mentir sur tes données personnelles et effectivement, c'est souvent illégal. Donc dans le cas d'entité relevant de l'état ou d'une assurance ou d'une banque, on ne ment pas. Pour tout le reste, tu peux mentir quand c'est possible.

Speaker1 : Parce que ce n'est pas toujours possible ?

Speaker2 : Ben oui! Si la piscine de Patin les oies réclame ta carte d'identité pour te délivrer ta carte d'abonné à tarif préférentiel, c'est difficile de mentir ensuite sur tes données personnelles.

Speaker1 : Un dernier conseil pour nos auditeurs ?

Speaker2 : Oui, et non des moindres : bien comprendre que nos données personnelles sont déjà dans la nature et ne pas croire ce qu'on lit dans ses e-mails ou SMS.

Speaker1 : Plus facile à dire qu'à faire.

Speaker2 : Oui mais il faudra s'y habituer.

Speaker1 : Bon, tu as parlé du point de vue du client, c'est-à-dire ce qu'on pouvait faire en tant que simple utilisateur, mais si je suis développeur, car je sais que beaucoup nous écoutent, qu'est-ce que je peux faire pour limiter ces fuites de données ?

Speaker2 : Et bien, comme tu ne maîtrises pas complètement la sécurité informatique de l'entreprise sur laquelle ta solution va être utilisée, le mieux, en tant que développeur, est de ne pas stocker de données confidentielles sur les utilisateurs. Ça évitera de mettre en danger ces utilisateurs si ton produit est victime d'une fuite de données.

Speaker1 : Oui car, si certains pirates veulent obtenir des données secrètes de certaines entreprises prestigieuses, d'autres veulent simplement extorquer le plus d'argent à des victimes.

Speaker2 : Oui tu as raison. Un premier type d'utilisation de ces données volées concernent surtout les états ou les entreprises concurrentes qui veulent savoir ce que fait tel autre état ou telle entreprise pour la contrer. Mais un deuxième type d'utilisation concerne effectivement les tentatives d’extorsion.

Speaker1 : Oui car en croisant toutes ces bases de données clients dérobées à droite à gauche, on peut arriver à faire croire aux victimes qu'on les connaît vraiment. Et j'en sais quelque chose! Heureusement que tu m'as rassurée.

Speaker1 : Donc il ne faut pas tomber dans le panneau! En partant du principe que nos données confidentielles sont déjà dans la nature et que les pirates y ont accès, on voit bien qu'il ne faut pas croire aux menaces qu'on nous envoie, même si le pirate semble connaître des informations personnelles sur nous. C'est juste pour nous faire chanter et nous extorquer de l'argent.

Speaker1 : Et tant qu'on parle de ne pas tomber dans le panneau, je crois que tu as encore une histoire passionnante à ce sujet à nous raconter.

##Bruit transition##

Speaker2 : Exactement Léa, et ça concerne un étrange email que m'a partagé un ami américain début septembre. Cet e-mail provenait d'un développeur malaisien qui lui proposait un arrangement assez étrange mais bien ficelé.

Speaker1 : D'ailleurs tu m'as expliqué hors antenne que Steeve Gibson l'avait évoqué dans l'épisode 990 de son émission Security Now.

Speaker2 : Oui c'est pour ça que je veux aussi alerter nos auditeurs, car le modus operandi utilisé est extrêmement bien rodé.

Speaker1 : Tu peux nous détailler ce modus operandi ? Tiens comment le développeur Malaisien a-t-il repéré ton ami développeur ?

Speaker2 : Tu as raison, commençons par le commencement. Alors mon ami américain, qu'on appellera Maurice pour préserver son identité, a été contacté par une personne de la manière suivante. Je te livre le texte du message.

Speaker3 : Salut Maurice, j'espère que tu va bien et que ça ne te dérange pas que je te contacte. Je m'appelle Lucas et je suis développeur généraliste en Malaisie. J'ai trouvé ton profil sur le site d'emploi usebraintrust.com. Et je voudrais te proposer une collaboration.

Speaker2 : Bon je passe le blabla, et il continue avec :

Speaker3 : Je cherche des boulots bien payés avec des entreprises ou clients aux États-Unis. Bien que ce soit possible depuis la Malaisie, en général ces entreprises cherchent des développeurs sur les même fuseaux horaires qu'eux. Malheureusement, en Malaisie on est sur du GMT plus huit, alors que les États-Unis sont entre les fuseaux GMT moins huit côté Pacifique et GMT moins cinq côté Est. Typiquement, pour des CDI ils ne prennent pas de développeurs en dehors des États-Unis.

Speaker1 : Bon allé, accouche!

Speaker2 : Tu vas voir, ça devient intéressant, écoute bien ce que Lucas écrit juste après.

Speaker3 : Donc je pense que la meilleure façon pour moi d'obtenir un boulot aux États-Unis, c'est de me faire passer pour un développeur basé aux États-Unis. Ça peut sembler risqué, mais ça ne le sera pas tant qu'on gardera notre collaboration 100% secrète. En outre, je n'ai pas besoin des informations sur ton identité.

Speaker1 : Ah oui, il n'y va pas par quatre chemins!

Speaker2 : Alors avant de continuer la lecture du message, je précise à nos auditeurs qu'Upwork et Toptal sont des plate-formes d'emplois pour indépendants. Et maintenant écoute comment Lucas propose de s'y prendre.

Speaker3 : Tout d'abord tu ouvres un compte sur Upwork ou Toptal, puis tu te connectes depuis ton deuxième ordinateur portable. Moi je me connecte à distance sur ce deuxième ordi et je cherche des missions. Tu reçois l'argent directement sur ton compte en banque, dès que je finis une mission. Tu prends ta commission et m'envoies le reste. Ce serait donc une collaboration non-technique et je te propose 15 à 20 pourcent pour toi et 80 à 85 pourcent pour moi. Pour les emplois en CDI, qui rapportent beaucoup plus que les missions pour indépendants, je candidaterais avec ton compte LinkedIn. Toi, tu passeras les entretiens et obtiendras les postes. Cependant, ça c'est pour une collaboration avancée, qui implique une solide confiance entre nous.

Speaker1 : Et pour les réunions, Lucas donne des précisions ?

Speaker2 : Oh oui, il indique :

Speaker3 : Je ferai le travail quotidien et toi tu participeras aux réunions. Je pourrai tout de même participer à ces réunions si les participants conviennent de désactiver leur caméra.

Speaker1 : Ce serait quand même super risqué pour ton ami, s'il acceptait.

Speaker2 : Oui, c'est pourquoi dans le cas d'un CDI, Lucas propose :

Speaker3 : Tu reçois ton salaire tous les 15 jours ou tous les mois et tu me reverses ma part après avoir déduit la tienne. Ce serait un mélange de collaboration technique et non-technique, et je propose qu'on fasse 20 à 25 pourcent pour toi, et 75 à 80 pourcent pour moi. Merci de me répondre par courriel si tu veux qu'on se cale un appel pour en discuter plus en détail ou si tu as d'autres idées pour la collaboration.

Speaker1 : Tout est possible bien sûr, ça peut être vraiment un Malaisien, mais ça me semble un peu gros quand même.

Speaker2 : Tu veux dire de mettre aussi clairement en avant l'appât du gain ?

Speaker1 : Oui tu n'as rien à faire, c'est moi qui ferai tout le travail technique et tu empocheras un cinquième d'un plein temps sans lever le petit doigt. Pour moi c'est lié à ces infiltrations nord coréennes qu'on a découvert ces derniers mois. Je n'ai plus en tête exactement comment ça s'est passé, mais peut-être peux-tu nous faire un résumé de ces infiltrations nord coréennes dans des entreprises occidentales.

Speaker2 : Oui, une des dernière histoire dont j'ai eu écho s'est passée en Juillet de cette année. Un ingénieur aux traits asiatiques a été embauché par une entreprise de formation en sécurité informatique appelée known4be. Cet ingénieur a passé avec succès tous les entretiens et toutes les vérifications sur son passé. Mais dès lors que l'ingénieur qui devait travailler à distance a reçu son Mac, il a commencé à charger des logiciels malveillants.

Speaker1 : Ah beh oui, chaque minute compte!

Speaker2 : Heureusement le logiciel de sécurité embarqué sur le Mac a détecté ces logiciels malveillants. Donc le service informatique a pu empêcher à temps que cet ingénieur ne compromette tout le système interne de l'entreprise. Pourtant l'attaquant ne manquait pas de toupet. Quand le service informatique l'a contacté pour lui demander des explications, le faux ingénieur a prétendu qu'il suivait les étapes de déblocage de son routeur suite à un problème de connexion.

Speaker1 : Attends, le faux ingénieur a reçu un Mac chez lui en Corée du Nord, et l'entreprise qui lui a envoyé ne s'est doutée de rien en écrivant l'adresse ? Ça parait complètement invraisemblable!

Speaker2 : Non, c'est beaucoup plus subtil que ça. Le faux ingénieur qui s'est avéré être un ressortissant nord coréen a utilisé une adresse basée aux États-Unis.

Speaker1 : Je ne comprends plus rien. Où était basé le faux ingénieur ?

Speaker2 : Il était basé en Corée du Nord, mais il s'est fait livré son ordinateur dans une ferme d'ordinateurs mules, basée aux États-Unis.

Speaker1 : Tu veux dire "mule" comme avec les personnes qui font passer de la drogue en la prenant sur eux ?

Speaker2 : Oui c'est le même principe et c'est le terme qu'ils utilisent dans leur article de blog.

Speaker1 : Donc si je résume. Un complice nord-coréen reçoit, aux États-Unis, dans une ferme d'ordinateurs, le Mac envoyé par l'entreprise. Il le connecte au réseau et l'employeur voit bien une connexion nationale étasunienne. Donc jusque là tout est cohérent pour l'employeur. Ensuite le complice sur place installe un logiciel de prise en main à distance, pour qu'ensuite le faux ingénieur basé en Corée du Nord puisse commettre son forfait à distance.

Speaker2 : Je pense que c'est tout-à-fait ça. Et c'est exactement au moment d'installer le logiciel de prise en main à distance que les alarmes se sont déclenchées.

Speaker1 : Il s'en est fallu de peu. Heureusement que l'entreprise était bien protégée. Une entreprise moins protégée ou sans détecteur de menaces aurait pu se faire avoir. Mais comment l'employeur a-t-il su que son entreprise était victime d'une infiltration de la Corée du Nord ?

Speaker2 : En fait, l'employeur a eu les bons réflexes, ce qui est rassurant car c'est une entreprise de formation à la sécurité informatique. Ils ont de suite contacté des collègues chez Google puis ont fait appel à la police fédérale, alias le FBI. Le FBI leur a alors confirmé qu'ils avaient affaire à un faux ingénieur de Corée du Nord.

Speaker1 : Donc en résumé, ce mode opératoire permet non seulement à la Corée du Nord d'accéder à des données sensibles de l'entreprise attaquée.

Speaker2 : Ça pourra toujours servir s'ils veulent monter une arnaque plus tard!

Speaker1 : Mais en outre ça leur permet aussi de faire entrer des dollars dans leur pays.

Speaker2 : Tu as raison de le préciser, car la Corée du Nord est très isolée sur le plan mondial. Par conséquent elle ne peut pas commercer. Mais avec cet argent frais gagné malhonnêtement, la Corée du Nord peut alors s'approvisionner en matériel étranger qu'elle paye avec les dollars.

Speaker1 : Attends, tu veux dire que grâce à ces infiltrations dans les entreprises américaines de la tec, la Corée du Nord parvient à financer son programme militaire ?

Speaker2 : Oui, le cyber finance donc le militaire!

Speaker1 : Ouah! Bon, ça c'était en Juillet, et ensuite il y a d'autres cas ?

Speaker2 : Oui un autre cas a été découvert cet automne. Mais avant d'en parler, je voudrais préciser, pour nos auditeurs francophones, que je laisserai sur notre site, la version francisée des conseils que livre l'entreprise victime, pour ne pas être infiltrée.

Speaker1 : Oui car rappelons que cette entreprise est spécialisée dans la formation à la sécurité informatique et qu'elle a contenu l'attaque en moins d'une demie heure. Tu peux peut-être d'ores-et-déjà nous livrer quelques-uns de ces précieux conseils ?

Speaker2 : OK pourquoi pas! Alors ils recommandent tout d'abord de renforcer les vérifications des candidats par des entretiens physiques ou en visio. Et en cas de doute pendant une visio le recruteur peut demander par exemple :

Speaker4 : Je vois que vous êtes sur Rennes. Où aimez-vous aller savourer une crêpe et laquelle choisissez-vous ?

Speaker1 : Ah oui, un ou une candidate qui vit sur Rennes pour de vrai n'aura pas de problème pour répondre à cette question. Par contre, un imposteur aura plus de mal à monter une réponse convaincante.

Speaker2 : Un autre conseil consiste à contacter par téléphone les anciens employeurs mentionnées dans le CV, de ne pas se contenter des adresses électroniques fournies par les candidats. Ensuite ils recommandent de surveiller les accès systèmes pour démasquer les activités suspectes. Et enfin, ils recommandent de sensibiliser les employés aux techniques de manipulation sociale et d'encourager les employés à signaler des comportements inhabituels. Nos auditeurs pourront retrouver les détails dans les notes de l'épisode.

Speaker1 : Je sens bien le nouveau métier qui va se créer maintenant : détecteur de faux employés Nord Coréens !

##Rire fort#

Speaker2 : Ah ah! L'avenir nous dira si tu as raison!

Speaker1 : Juste une précision. Tu crois que c'est à cause de ces attaques nord coréennes que de plus en plus d'entreprises veulent limiter le recours au télétravail ? Je pense à Ubisoft qui a entraîné une levée de bouclier en voulant ramener ses employés dans ses locaux.

Speaker2 : Non je ne pense pas que cette demande de retour au travail en présentiel est dû aux tentatives d'infiltrations Nord Coréennes. Sinon les employeurs l'auraient dit.

Speaker1 : Bon on a un peu digressé, tu mentionnais une autre infiltration nord coréenne ?

Speaker2 : Oui tout-à-fait. Mais celle-ci a abouti cette fois. Elle a été révélée en octobre dernier, et a touché le monde de la crypto. La chaîne de blocs Cosmos est concernée. Elle a été noyautée de l'intérieur depuis au moins 2023 voire 2021 par des travailleurs Nord Coréens.

Speaker1 : Et quels problèmes ce genre d'infiltration dans les chaînes de blocs pose-t-il ?

Speaker2 : Et bien, ces travailleurs Nord Coréens infiltrés peuvent ajouter des portes dérobées, ou des vulnérabilités dans le code pour rendre la crypto piratable. Et la seule manière ensuite d'enlever ces failles est de conduire un audit complet du code.

Speaker1 : Mais quel est le but pour ces Nord Coréens ? Pourquoi ajoutent-ils des failles dans le code des chaînes de blocs ?

Speaker2 : Ils veulent simplement pouvoir se faire de l'argent. Imagine que tu fasses un paiement avec la crypto Cosmos, et qu'ensuite tu connaisses une astuce pour te rembourser ce même montant. Tu achètes alors tout ce que tu veux gratuitement.

Speaker1 : Mais je ne comprends pas. L'immutabilité d'une crypto-monnaie ou d'une chaîne de blocs est la pierre angulaire de cette technologie. C'est-à-dire que l'immutabilité empêche toute altération du registre des transactions. Donc tu ne peux pas effacer une transaction.

Speaker2 : Tu as raison, c'est le fonctionnement théorique de la chaîne de blocs. Mais ensuite tu as l'implémentation logicielle qui, si elle amène des failles de sécurité, peut diverger du fonctionnement théorique souhaité.

##Bruit de quelqu’un qui tombe de sa chaise##

Speaker2 : Qu'est-ce qui se passe, j'ai entendu un bruit sourd ?

Speaker1 : Oh c'est rien! Je suis tombé de ma chaise! J'étais tellement étonnée!

Speaker2 : Ah bon ? Alors accroche toi bien maintenant, car la Corée du Nord s'est spécialisée dans les cryptos. D'ailleurs le groupe de cyber pirates Nord coréens nommé Lazarius avait déjà détourné près de 600 millions d'Euros en 2022.

Speaker1 : Avec l'essor des cryptos tel qu'on le voit actuellement, s'il y a des failles un peu partout, ça va leur faire une sacrée cagnotte.

Speaker2 : Oui, mais au détriment des investisseurs honnêtes qui ont placé toutes leurs économies dans les cryptos.

Speaker1 : Et qui peuvent tout perdre du jour au lendemain si la Corée du Nord le décide.

Speaker2 : Comme tu dis, c'est vertigineux!

Speaker1 : Et bien, encore merci Charlie pour ton éclairage précieux sur tous ces sujets. On se retrouve le mois prochain ?

Speaker2 : Avec plaisir ma chère Léa! Mais le mois prochain ce sera Noël, donc on se retrouvera plutôt en janvier!

Speaker1 : Exact, j'avais oublié Noël! Et je rappelle à nos auditeurs qu'ils peuvent deviner quelles voix nous imitons dans nos épisodes, et gagner des super cadeaux.

Speaker2 : Ah oui comme des comptes nettoyeurs bénévoles Bye Bye Crottoir! J'en ai des étoiles plein la tête.

Speaker1 : Oui, ça fait rêver! Alors comme c'est un peu difficile ce mois-ci, je donne un indice sur les voix imitées. On est le jour de l'élection américaine. Je répète : on est le jour de l'élection a-mé-ri-cai-ne.

Speaker2 : Avec ton indice ce sera plus facile! Et comme toujours, chers auditeurs et chères auditrices, n'hésitez pas à nous laisser vos commentaires et à partager cet épisode avec vos amis pour les sensibiliser aux dangers cachés derrière nos technologies quotidiennes.

Speaker1 : Oh, et j'allais oublié, vous pouvez aussi nous retrouver sur Spotify et Youtube Music! On est Failles Sécu! Ciao Charlie!

Speaker2 : Salut, à bientôt ma Léa! Et que Dieu bénisse la cyber-sécurité.

##Jingle Fin##