Failles Sécu

Transcription[1]

Épisode 14 : Mots de Passe : la fin du calvaire ?

Léa : Bonjour à toutes et à tous et bienvenue dans ce quatorzième numéro de Faille Sécu, l'émission qui vulgarise la cybersécurité et parle de ses répercussions concrètes dans votre quotidien. Je suis Léa et je serai votre guide tout au long de cet épisode un peu spécial, je l'assume, intitulé « Mots de Passe : la fin du calvaire ? ». **[JINGLE]** Bien le bonjour très chère Charlie, je suis heureuse qu'on se retrouve une nouvelle fois pour parler cybersécurité.

Charlie : Très clairement ça faisait un bon bout de temps qu'on n'avait pas enregistré, alors quelle joie de me retrouver de nouveau sur ce plateau avec toi ! Tu as bien fait de parler de numéro spécial, car ce n'est pas vraiment le sujet qui était prévu, mais comme il est brûlant, j'ai crois profondément qu'il était nécessaire de l'insérer dans le fil des épisodes prévus. On va donc voir pourquoi la fin du calvaire est peut-être proche pour de nombreux utilisateurs qui se connectent quotidiennement à un ordinateur pour leur travail. Une fois ce sujet traité, on reprendra le cours normal de nos émissions.

L : Dois-je comprendre qu'on est parti pour quelques épisodes ?

C : Mmm, je l'espère, c'est comme ça que c'est prévu en tout cas.

L : Gé-nial ! Au fait, excuse-moi mais on a de nouvelles voix on dirait ?

C : Exact ! Car un auditeur perspicace de Toulouse a découvert les voix imitées dans l'épisode précédent. C'était bien celles d'Élise Lucet et Fabrice Drouelle. En conséquence on en utilise des nouvelles pour cet épisode.

L : Oui car je rappelle que, dans l'épisode précédent, tu as décrété que tu allais investir 1 M€ pour offrir à nos auditeurs une écoute impeccable. Et tu t'es engagée à changer nos voix dès que les auditeurs devinent les célébrités imitées. Franchement, tu sais que tu n'es pas obligée de tenir parole là-dessus et qu'on n'est pas non plus obligées de venir enregistrer les émissions dans un des studios d'enregistrement les plus renommés de Paris, décoré aux couleurs de Failles Sécu, et dont les prestations doivent coûter un joli bras ?

C : Oh mais si, ça me fait plaisir tu sais et je l'assume totalement. Très clairement, je veux que nos auditeurs vivent une expérience hors du commun lorsqu'ils écoutent notre émission. C'est un peu notre « quoi qu'il en coûte » à nous ! Et ça contribue à donner à la cybersécurité une image positive et à ancrer encore plus efficacement les bonnes pratiques et les règles d'une bonne hygiène informatique chez nos auditeurs et auditrices.

1 Post-correction : Il peut arriver que des termes incorrects se glissent dans cette transcription de l'épisode. Ces termes incorrects sont alors ~~barrés~~ et suivis du terme plus approprié surligné.

L : Très clairement, avec ces mots merveilleux, tu m'offres une transition parfaite pour amener notre sujet du jour ! Car aujourd'hui on va s'intéresser aux nouvelles recommandations du NIST américain relatives aux bonnes pratiques en terme de choix de mot de passe. Tiens qu'est-ce que c'est déjà qu'un bon mot de passe, Charlie ?

C : OK, alors un bon mot de passe ce n'est déjà pas un mot du dictionnaire, mais plutôt une suite de chiffres et de lettres (on parle de « caractères ») qu'on ne peut pas trouver facilement, donc qui est le plus aléatoire possible.

L : Tu veux dire que notre mot de passe doit apparaître comme s'il avait été généré au hasard ?

C : Oui c'est ça. Aux yeux du pirate qui cherche à craquer notre mot de passe, celui-ci doit apparaître comme complètement aléatoire de manière à ce qu'il ne puisse pas le deviner. Par contre, pour celui qui créé le mot de passe, l'agencement des chiffres et des lettres n'est pas dû au hasard car il doit le retenir !

L : Alors quelles sont ces recommandations du NIST ? Et qui est le NIST au fait ? C'est l'équivalent de notre ANSSI, l'Agence Nationale de la Sécurité des Systèmes d'Information ?

C : Oui, en quelque sorte. Le NIST est une agence gouvernementale américaine, l'Institut National des Normes et de la Technologie. Il développe des normes, et publie des guides détaillés pour assurer la sécurité et la fiabilité des technologies. C'est un de ces guides là qui vient d'être mis à jour et qui traite de cryptographie et d'utilisation de mots de passe sûrs.

L : Donc ce sont les américains du NIST qui expliquent au monde entier comment bien choisir ses mots de passe ? Et ce sont leurs recommandations qui sont ensuite édictés sans discernement comme règles par tous les services informatiques du monde entier et qui pourrissent parfois le quotidien des collaborateurs au travail ?

C : Je te sens remonté contre le NIST ! Tu veux en parler ?

L : Oui c'est affreux. La réalité, elle est là, des services informatiques de plein de boites dans le monde imposent à leurs utilisateurs de changer de mot de passe très fréquemment car le NIST l'a mis dans son précédent guide. Alors tous les mois, il faut changer de mot de passe en arrivant au boulot le matin, et il faut que ce mot de passe fasse une certaine longueur, et qu'il soit complètement différent non seulement du précédent mais aussi des 5 ou 10 derniers. Bref ces anciennes recommandations sont un enfer, c'est clair, net et précis. On le sait très bien, elles ajoutent une charge mentale infernale pour les utilisateurs. Moi je te le dis, c'est en partie à cause d'elles que s'est créé ce climat délétère entre les services informatiques et leurs utilisateurs qui se sentent harcelés. Et donc maintenant ils ont sorti leur V2 ?

C : Oui et tu vas voir qu'ils ont mis de l'eau dans leur vin.

L : Tu veux dire qu'ils vont permettre aux services informatiques du monde entier de se rabibocher avec leurs utilisateurs ?

C : Je pense que oui, évidemment. Les recommandations auxquelles tu fais référence étaient un peu trop extrêmes.

L : Ah parfait ! Alors qu'elles sont ces recommandations ? Et où peut on les lire.

C : Et bien, on peut les lire sur leur site, et je mettrai le lien vers le document en anglais sur notre à la page de cet épisode. Le document nommé SP 800-63B est daté du 26 Août de cette année (26 Août 2025) et fait une bonne centaine de pages.

L : Ouarf ! On en a pour un dizaine d'épisodes à couvrir ce document !

C : Oui, le document est très vaste, mais en réalité les recommandations qui nous intéressent se trouvent au chapitre 3.1.1.2 intitulé « Vérificateurs de mots de passe ». On peut les résumer en 8 recommandations qui font sens et qui sont assez faciles à mettre en place :

1) Tout d'abord, le mot de passe doit faire 15 caractères minimum s'il est le seul moyen utilisé de s'authentifier et on peut le réduire à 8 caractères s'il est utilisé de pair avec d'autres moyens d'authentification.

L : Tu veux dire que si pour me connecter à un site quelconque on me demande seulement un mot de passe, alors il faut que celui-ci soit assez long, tandis que s'il me faut aussi utiliser par exemple mon téléphone pour confirmer que c'est bien moi, alors le mot de passe peut être réduit ?

C : C'est ça oui.

L : Ok je prends. On continue ?

C :

2) Alors leur deuxième recommandation est d'autoriser des mots de passe d'au moins 64 caractères.

L : Soyons sérieux, 64 caractères ? Mais c'est super long pour un mot de passe. Je ne comprends pas trop l'intérêt d'une telle recommandation. Il faut être fou pour retenir un tel mot de passe et le taper tous les matins quand tu commences le boulot !

C : Pas forcément, et ce n'est pas une obligation, c'est juste une possibilité qui doit être offerte à l'utilisateur. Car rien ne t'empêche de choisir une phrase comme mot de passe. Tu peux choisir ce qui te passe par la tête à ce moment là, par exemple : « Aujourd'hui il fait beau, je vais donc pouvoir me baigner dans la Seine ». Tu vois c'est pas difficile à retenir, mais ça fait déjà 71 caractères, espaces compris. Donc en tant qu'administrateur informatique, si tu veux faciliter la vie des utilisateurs, tu leur permets de choisir un mot de passe aussi long qu'ils le souhaitent dans la limite du raisonnable. C'est le sens de cette recommandation du NIST.

3) Ensuite leur troisième recommandation concerne justement l'autorisation de tous les caractères imprimables dans le mot de passe, y compris les lettres accentuées, les caractères de ponctuation, les espaces, etc …

L : Ah oui parce que parfois on ne nous autorise pas à utiliser les accents, cédilles et compagnie. Il n'y a rien de plus horripilant. En plus c'est juste à cause du concepteur du site qui n'a pas voulu se donner la peine de prendre en charge autre chose que les caractères américains standards.

C : Et oui, tu as raison de le souligner. Et c'est dû au fait que l'informatique a été longtemps pensée en anglais seulement. Pense au mot-clés dans les langages de programmation. Tout est en général en anglais (« for », « if », « else » « function », ...). Donc c'est une bonne chose que le NIST mette dans ces recommandations d'accepter tous les caractères. Ça demande effectivement plus de travail pour les développeurs, mais à l'heure de l'Intelligence Artificielle, ce n'est plus un problème, c'est quelque chose que l'IA fait sans problème.

4) Alors on passe à la quatrième recommandation du NIST qui demande de ne pas obliger l'utilisateur à combiner plusieurs sortes de caractères dans son mot de passe.

L : Ouah, j'adore cette recommandation ! Enfin on n'aura plus à mélanger les majuscules, les minuscules, les chiffres, les signes de ponctuation, sauf ceux qu'on ne doit pas mettre ! Ah vraiment génial.

C : Oui et c'est logique, car il vaut mieux un mot de passe long rien qu'avec des lettres qu'un mot de passe court avec des chiffres et des lettres. Et pour s'en convaincre, on peut aller voir sur le site grc.com de Steve Gibson, à la page qu'il appelle littéralement « La botte de foin des mots de passe » (ou « password haystack » en anglais).

L : Attends, on va le faire en direct: g r c . com / haystack.

C : Eh excellente idée Léa ! On va donc comparer en direct le temps qu'il faudrait à un pirate pour deviner un mot de passe de 8 caractères comprenant des majuscules, des minuscules, de la ponctuation, et des chiffres, comme c'était la règle jusqu'à présent. Et on va comparer ça au temps qu'il faudrait au même pirate pour trouver un mot de passe plus long mais constitué seulement de lettres minuscules et d'espaces, comme c'est maintenant autorisé.

L : Donc j'ai tapé le mot « B0nj0ur ! » avec une majuscule, les « o » remplacés par des « zéros », et un point d'exclamation à la fin. Et d'après le calculateur du g r c, si le pirate utilise du matériel dédié performant qui peut tester hors-ligne des milliers de milliards de mots de passe à la seconde, il lui faudrait au maximum 1 minute et 7 secondes pour découvrir ce mot de passe de 8 ~~lettres~~ caractères. C'est quand même assez rapide. On a une idée du matériel nécessaire pour de telles performances ?

C : D'après un test de carte graphique trouvé par ChatGPT, et réalisé il y a trois ans, une carte graphique moderne de type RTX 4090 peut tester plus d'une centaine de milliards de mots de passe par secondes. Donc il en faudrait une dizaine pour arriver aux performances supposées par le calculateur de Steve Gibson.

L : À 1000 ou 2000€ la carte graphique, le pirate doit être sacrément fortuné !

C : Oui ou être soutenu par un état. Pense aux groupes de pirates soutenus par les Russes, les Chinois, les Iraniens, ou les Nord-coréens. Et il doit y avoir des groupes équivalents de l'autre côté, soutenus par les américains, et les occidentaux en général. Et ces groupes là possèdent déjà l'infrastructure de toute façon, et comme ces groupes sont plus ou moins rattachés à l'armée, le pognon coule à flot. Par conséquent, on peut imaginer que des pirates étatiques sont tout à fait en capacité de deviner un mot de passe de 8 caractères aussi vite.

L : À propos, tu peux préciser pourquoi on dit que cette durée pour trouver le mot de passe est une durée **maximale** et qu'en général le pirate mettra beaucoup moins de temps que ça à trouver le mot de passe ?

C : Très bonne question Léa. Effectivement, la durée annoncée par le calculateur en ligne est le temps maximum qu'il faudrait au pirate s'il trouvait le mot de passe juste à la fin après avoir cherché de manière naïve toutes les combinaisons possibles. Par exemple, il commence par « a » puis « b », puis « c » jusqu'à « z » puis « a1 », « a2 », « a3 », …, essaye « bonjour », et le dernier mot qu'il essaie est « B0nj0ur! ». Dans ce cas, il n'a pas eu de chance et a dû tester l'ensemble des combinaisons possibles de chiffres, lettres, signes, avant de tomber sur ton mot de passe. Mais dans la vraie vie, le pirate est malin et il va commencer en priorité par les mots de passe les plus connus (car il n'en est pas à son coup d'essai et s'est donc déjà constitué une base de données des mots de passe les plus fréquemment utilisés), dont fait probablement parti ton « B0nj0ur! » avec des « zéros » à la place des « o ». Ensuite il va essayer tous les mots du dictionnaire dans toutes les langues et toutes les variations de ces mots où des lettres ont été remplacées par des chiffres ou des symboles. Donc si ton mot de passe est là dedans, il sera trouvé en à peine quelques secondes.

L : C'est pour ça qu'on veut que le mot de passe soit le plus aléatoire possible ?

C : Oui c'est tout-à-fait exact. On parle même d'entropie d'un mot de passe, c'est-à-dire l'ensemble des combinaisons possibles d'un mot de passe, exprimées en bits. Par exemple si tu n'utilises que des lettres minuscules dans ton mot de passe de 2 lettres, tu auras 26 x 26 soit 676 possibilités ou une entropie d'un peu plus de 9 bits.

L : Donc si je comprends bien, l'entropie reflète la force d'un mot de passe, ou sa propension à résister à une attaque pour le deviner.

C : Oui c'est assez vrai. Mais l'entropie ne mesure pas complètement la force ou la résistance d'un mot de passe. L'entropie donne juste une idée de la quantité de hasard contenue dans un mot de passe d'une longueur donnée si chaque caractère est choisi vraiment au hasard. Et c'est ce choix de caractères vraiment au hasard qui est le plus important.

L : OK je veux bien te croire, mais je pense qu'avec un exemple, ce serait encore plus clair. Tiens par exemple, si je choisis comme mot de passe, le mot le plus long de la langue française, à savoir « anticonstitutionnellement ».

C : Et bien partons sur cet exemple. Ton mot de passe, « anticonstitutionnellement » a, à première vue, une entropie énorme car il est très long (son entropie fait 122 bits si on fait les calculs, ce qui représente un nombre de possibilités à 37 chiffres). Mais en fait, comme c'est un mot du dictionnaire et qu'il y a environ 63 000 mots dans le Larousse, ça réduit le nombre de possibilités et aussi l'entropie à un peu moins de 16 bits. Mais ce n'est pas fini, car comme le pirate prédit que l'utilisateur qui se croit malin va probablement utiliser le mot le plus long de sa langue, le pirate va inclure ce mot dans sa base des 100 mots de passe les plus utilisés, à tester en priorité. Donc finalement, le pirate va essayer ce mot de passe dès le début et comme ça ne fait que 100 possibilités ou une entropie d'un peu plus de 6 bits, il va le trouver encore plus vite que le mot de

passe de 2 lettres minuscules qu'on a imaginé tout-à-l'heure qui avait une entropie d'un peu plus de 9 bits.

L : Excuse-moi mais je ne te suis plus du tout. Tu es en train de dire qu'un mot de passe de 26 lettres (« anticonstitutionnellement ») est moins résistant à l'attaque d'un pirate malin qu'un mot de passe de 2 lettres. Comment cela se fait-ce ?

C : La différence est que les 2 lettres sont choisis complètement au hasard, c'est ça la clé ! Donc le pirate est obligé de tester l'ensemble des 676 possibilités, tandis que comme « anticonstitutionnellement » est dans la liste des 100 mots de passe du pirate à tester en priorité, il aura seulement 100 essais à effectuer.

L : Donc il trouvera plus vite « anticonstitutionnellement » que « zf » par exemple. Mais pourquoi « anticonstitutionnellement » serait dans sa liste de mots de passe à tester en priorité ?

C : Ah ça, ça vient du fait que de nombreuses bases de données d'entreprises mal protégées ont été piratées (et malheureusement le sont encore), c'est-à-dire que des pirates sont parvenus à y accéder, à les copier et à publier leur contenu. On se souvient, de Picard, de Free, et des autres qu'on avait évoquées dans des émissions précédentes. Ces bases de données contiennent souvent des listes d'utilisateurs avec leurs mots de passe en toutes lettres et en clair. Donc les pirates du monde entier n'ont plus qu'à analyser toutes ces bases de données, et à noter quels sont les mots de passes les plus fréquemment utilisés. C'est comme ça qu'ils constituent leurs listes de mots de passe à tester prioritairement.

L : Il n'y a que les pirates qui constituent ces listes ?

C : Excellente question ma Léa ! Et non, ils ne sont pas les seuls. En effet, pour le bien de l'humanité, d'autres personnes analysent aussi ces bases de données lorsqu'elles sont publiées dans les forums ou sur l'internet caché (le fameux dark web). Ils mettent ensuite à disposition de tout-un-chacun le résultat de leurs analyse ssous forme d'une interface conviviale où l'on peut taper son mot de passe et voir s'il est déjà apparu dans une des bases de données piratées, et qui est donc connu par les pirates et par conséquent qu'il ne vaut mieux pas utiliser.

L : Ah oui, c'est le fameux site anglais « ai-je été piraté » ! Et si je teste en direct, « an ti cons ti tu tion nelle ment », le résultat apparaît immédiatement … Ouh ! Ce mot de passe apparaît dans plus de 1500 bases de données piratées. Ah c'est pourquoi il ne faut jamais réutiliser un mot de passe.

C : Exactement, c'est une règle cardinale en terme de sécurité, et tu fais bien de le souligner. Chaque site doit avoir son propre mot de passe.

L : Et maintenant, si j'ai bien compris, la force d'un mot de passe est donnée par son entropie si tous les caractères sont choisis au hasard, sans liens apparents les uns avec les autres. S'il n'y a pas assez de hasard dans le choix des caractères et que par voie de conséquence les caractères sont prévisibles par le pirate, alors la force ou la résistance du mot de passe peut devenir dérisoire.

C : Bravo, tu as parfaitement résumé le concept d'entropie !

L : Par contre, je n'ai pas bien compris comment on passe d'un nombre de possibilités à une entropie en bits. D'où viennent ces bits, je suis un peu confuse là dessus ?

C : Oh c'est très simple : les bits sont juste l'unité de mesure de l'entropie. Avec 1 bit d'entropie tu peux avoir 2^1 possibilités soit 2 possibilités, si tu as 2 bits d'entropie, tu peux en avoir 2^2 soit 4 possibilités, si tu as 3 bits d'entropie, tu peux avoir 2^3 soit 8 possibilités, et ainsi de suite. 10 bits d'entropie correspondent à 1024 possibilités (2^{10}).

L : Ah, OK donc c'est juste le nombre de possibilités exprimées en binaire. C'est bon j'ai compris. Tu es vraiment la reine des explicatrice Charlie ! Et alors j'imagine qu'un mot de passe de 2 lettres, comme « zz », qui a une entropie de 9 bits n'est pas suffisant. Mais a-t-on une idée de l'entropie minimale requise pour un bon mot de passe bien sécurisé ?

C : Pour répondre à ta question, on regarde combien de temps il faudrait à un pirate pour trouver ton mot de passe, s'il avait à sa disposition le meilleur matériel d'attaque disponible, c'est-à-dire du matériel capable de tester des milliers de milliards de mots de passe par seconde.

L : Ah oui, comme le suppose Steve Gibson sur son site dont on a parlé précédemment.

C : Exactement. Donc, à cette vitesse de calcul, dans le meilleur des cas, pour un mot de passe avec une entropie de 40 bits, la mathématique nous donne 1 seconde de résistance. Pour 50 bits d'entropie, on est à presque 19 minutes, pour 60 bits on est à un peu plus de 13 jours, ce qui reste toujours faisable, puisqu'en moyenne le pirate mettra la moitié de ce temps à découvrir le mot de passe. À partir de 70 bits d'entropie on commence à parler en années (plus de 37 ans), et pour 80 bits on entre dans l'inimaginable avec des durées exprimées en dizaines de milliers d'années.

L : Bon, on ne va pas faire semblant, un mot de passe avec une entropie de 80 bits serait incraquable. A-t-on un moyen de savoir à combien de caractères aléatoires ces 80 bits d'entropie correspondent ?

C : Oui c'est possible de le savoir, et il faut alors poser quelques bases. Si tu considères toutes les lettres majuscules et minuscule disponibles sur un clavier américain (c'est-à-dire sans accents ni cédilles), ainsi que tous les chiffres et les 32 symboles communs, tu as un ensemble de 94 caractères soit une entropie de 6,5 bits par caractère. Donc pour atteindre 80 bits d'entropie avec ce panel de caractères, il faut entre 12 et 13 caractères parfaitement aléatoires.

L : Donc le NIST va plus loin, puisqu'il conseille un minimum de 15 caractères.

C : Oui il a certainement pris un peu de marge. Mais n'oublie pas qu'il conseille de ne pas imposer à l'utilisateur de mélanger plusieurs types de caractères (majuscules, minuscules, chiffres, etc …). Donc si l'utilisateur ne choisit pour son mot de passe que des lettres et des chiffres (donc avec une entropie par caractère plus réduite d'environ 5,2) on est à a peu près 15-16 caractères.

L : Bon très clairement, on a bien débordé de la liste des recommandations du NIST, mais je pense que maintenant c'est bien plus clair pour tous ceux et celles qui nous écoutent. Donc on a vu 4 recommandations du NIST, quelle est la cinquième ?

C :

5) Alors la cinquième recommandation du NIST conseille de ne pas demander à l'utilisateur de changer son mot de passe régulièrement sauf si on a des preuves que le mot de passe a fuité.

L : Ouah mais c'est merveilleux, on n'aura plus à changer son mot de passe tous les 4 matins avant de pouvoir utiliser son ordinateur ! Tu sais, ça paraît pas comme ça, mais ça va diminuer la charge mentale des collaborateurs d'une entreprise. Et je suis sûre que ça va améliorer grandement les relations entre le service informatique et les autres services.

C : Tant mieux si ça arrive !

6) La sixième recommandation demande de ne pas permettre à l'utilisateur de stocker des indices pour retrouver son mot de passe. Par exemple, « Le mot de passe commence par une majuscule » ou « C'est le nom de mon premier chien ».

7) Dans le même style, la septième recommandation conseille de ne pas encourager l'utilisateur à utiliser des « questions de sécurité » ou « basées sur la connaissance » lors de la création ou la modification de son mot de passe. Par exemple « Quel est le nom de votre grande tante maternelle au troisième degré » ou « quelle est la ville de naissance de votre mère ».

L : Ah oui, je le dis, c'est inacceptable de telles questions. Car ces informations, le pirate peut les trouver sur internet, sur les réseaux sociaux par exemple, ou déjà les avoir en sa possession d'un précédent piratage.

C : Très juste !

8) Et enfin, la huitième et dernière recommandation conseille de demander le mot de passe complet (pas seulement un bout) et de le vérifier dans sa totalité (sans le tronquer par exemple).

L : Pourquoi est-ce si important ?

C : Eh bien il faut que l'utilisateur entre son mot de passe complet, car si on l'autorise à n'entrer que les 4 premiers caractères ou qu'on ne vérifie que ces premiers caractères, alors on diminue sa résistance.

L : Ah oui, on en revient à l'entropie du mot de passe.

C : Exactement Léa ! Si tu autorises l'utilisateur à n'entrer que les premiers caractères, alors tu limites l'entropie à une vingtaine de bits. Et si ça t'est autorisé, ça l'est aussi pour le pirate qui essaye d'accéder à ton compte. Et c'est bien que le NIST précise aussi qu'il faut vérifier tous le caractères, car certains sites ne stockaient qu'une portion du mot de passe, sans te le dire. Donc tu mettais un mot de passe super long, mais le site ne stockait que les 8 premiers caractères car il estimait que c'était suffisant. Donc toi, tu te croyais en sécurité, mais ce n'était que de la poudre aux yeux.

L : Donc si tu me permets de résumer ces recommandations du NIST sur les mots de passe, on peut dire que l'institut américain conseille désormais de laisser beaucoup plus de liberté à l'utilisateur dans le choix de son mot de passe, et franchement c'est une bonne chose. Il conseille aussi de ne pas l'obliger à inclure certains types de caractères mais à l'autoriser à le faire s'il le souhaite. D'autre part, le NIST recommande d'utiliser un mot de passe de 15 caractères minimum s'il est utilisé seul, ou 8 s'il est utilisé de pair avec un autre moyen d'authentification. Enfin le NIST recommande de ne plus obliger l'utilisateur à changer régulièrement son mot de passe, et d'arrêter d'employer des méthodes qui affaiblissent le mot de passe. En conséquence, on dirait que c'est bel et bien la fin des règles compliqués avec les mots de passe, donc la fin du calvaire pour de nombreux utilisateurs qui pourront définir leur mot de passe sûr beaucoup plus sereinement ? Euh, je te vois faire la grimace. Ça n'en est pas fini ?

C : Si tu as raison, mais ces recommandations du NIST sont assez récentes, il faut donc qu'elles arrivent aux oreilles des responsables des services informatiques et qu'ils les mettent en place dans leurs entreprises. Par conséquent, ça risque de ne pas être immédiat, mais je ne doute pas que les utilisateurs bien informés, dont nos auditeurs et auditrices, ne manqueront pas de mettre la pression sur leur service informatique pour qu'il ne tarde pas à ~~diffuser~~ appliquer ces nouvelles règles !

L : Ah, ça me rassure ! Et sinon, Toi ma chère Charlie, as-tu des recommandations complémentaires pour nos auditeurs et auditrices, bien informé(e)s ?

C : Oui, en pratique, je recommande à tous ceux qui nous écoutent d'utiliser un gestionnaire de mots de passe. Il en existe plein, et il y en a même un intégré au navigateur Firefox. Comme ça, c'est le gestionnaire qui s'occupe de vous trouver des mots de passe parfaitement au hasard, pour chaque site qui vous le demande, et ensuite ce gestionnaire s'occupe de préremplir les formulaires d'authentification automatiquement lorsque vous visitez ces sites. En outre, l'autre bénéfice d'utiliser ces gestionnaire de mots de passe, est qu'ils vous protègent en cas d'attaque par hameçonnage.

L : Ah oui, le faux courriel du site XYZ, plus vrai que nature car rédigé par une IA et qui te propose de cliquer sur un lien pour te connecter.

C : Dans ce cas, si tu te fais avoir et cliques sur le lien, tu vas bien atterrir sur le faux site qui pourra paraître vrai à tes yeux, mais pas à ceux du gestionnaire de mots de passe qui aura reconnu le « I » majuscule à la place du « l » dans l'adresse et ne préremplira pas le formulaire de connexion. Dans ce cas, ça doit nous mettre la puce à l'oreille. Il ne faut pas insister et taper l'adresse du site manuellement, comme on le fait habituellement. La supercherie sera découverte facilement.

L : Un autre conseil ?

C : Oui, et celui là est le plus important : ne jamais réutiliser le mot de passe d'un site pour un autre. C'est vraiment la base. Je le redis, ne jamais réutiliser d'un site pour un autre. Avec un gestionnaire de mots de passe, cela ne peut plus arriver car c'est lui qui génère un mot de passe pour chaque site. Par conséquent, il n'y a pas de lien entre tous nos mots de passe et tu es tranquille en cas de piratage sur un site.

L : Mais attends, pourquoi est-ce si important de ne pas réutiliser le mot de passe d'un site sur un autre site ? S'il est sécurisé, il n'y a pas de risque, non ?

C : Oh que si. Et tu vas tout de suite comprendre pourquoi. Quand un site est piraté et que les mots de passe de ce site sont découverts, le pirate obtient aussi les identifiants associés. Par exemple le site de vente « mes-surgelés.fr » est piraté. Le pirate obtient alors plein de données dont le mot de passe « singe 123 » associé au compte « tartampion@gmail.com ». Donc la première chose que va faire le pirate est d'essayer de ce connecter au compte gmail de tartampion avec le mot de passe qu'il vient de glaner et ses variations (par exemple avec une majuscule, avec un « 1 » à la place du « i », etc ...). Et si tartampion utilise toujours le même passe, alors le pirate peut accéder à son compte gmail et c'est le début des problèmes pour tartampion qui peut se faire voler son identité, et l'accès à tous les comptes associés à cette adresse électronique ! En outre ses accès seront revendus sur l'internet caché pour lancer de nouvelles attaques.

L : Et j'imagine que si le pirate ne parvient pas à se connecter au compte gmail de tartampion, il va quand même garder ce mot de passe et l'essayer pour d'autres sites. Car les sites étant disponibles 24h / 24 , 7j / 7 , les pirates peuvent lancer leurs attaques en continu depuis chez eux vers le monde entier. Ça ne leur coûte rien en outre, car ce sont juste des programmes qui tournent de manière autonome. Grâce à ton explication, maintenant je comprends parfaitement pourquoi il faut un mot de passe différent pour chaque site, ce qui ne pose pas de problème quand on utilise, comme tu le préconises, un gestionnaire de mots de passe qui se charge d'en trouver un nouveau pour chaque site que tu visites. Mais au fait, quand on choisit un gestionnaire de mots de passe, il faut aussi définir un mot de passe principal, ultra solide à très haute entropie qui protègera tous les autres mots de passe. Comment le choisit-on ?

C : C'est on ne peut plus exact ! Le mot de passe principal du gestionnaire de mots de passe ne doit pas être choisis à la légère, car s'il est deviné, le pirate aura accès à tous nos comptes. Ce mot de passe doit donc être « ultra résistant » comme tu dis !

Alors pour définir un mot de passe fort, et qu'on peut retenir, je conseille toujours de s'imaginer une phrase et de prendre les premières lettres de chaque mot. Par exemple si on choisit la phrase « On a fait un super podcast aujourd'hui,[virgule] il me tarde d'enregistrer le prochain ! [point d'exclamation]», ça fera « O » majuscule pour « On », puis « a », puis « f » pour « fait » et on continue jusqu'à la fin, sans oublier la ponctuation quand on en rencontre. Donc ici ça fera « O » majuscule, « a f u s p a » « apostrophe » « h » « virgule » « i m t d » « apostrophe » « e l p» « point d'exclamation ». Ce qui fait 18 caractères aléatoires, faciles à retenir. Après si tu ne veux pas inclure les apostrophes, c'est à toi de voir.

L : Et bien voilà je crois qu'avec tes conseils, nos auditeurs et auditrices sont prêts à affronter sereinement les attaques des pirates.

Comme toujours, c'était une émission passionnante Charlie. Tu nous as encore expliqué la cybersécurité en des termes simples qu'on a tous pu comprendre, tu mérites vraiment ton titre de vulgarisatrice en chef !

C : Tu vas me faire rougir Léa ! C'est ma passion et j'apprécie beaucoup de la partager avec nos auditeurs et auditrices.

L : J'ai déjà hâte qu'on se retrouve pour notre prochaine émission. Tu crois qu'on aura des nouvelles voix ?

C : Ah ça, en réalité, c'est nos auditeurs qui le décideront, s'ils découvrent quelles voix on imite.

L : Oui et je rappelle l'adresse pour nous écrire « failles au pluriel sécu tout attaché @ intracherche.fr ». Et on connaît déjà le thème de notre prochaine émission ?

C : Oui maintenant qu'on a traité ce sujet brûlant du NIST, on va pouvoir reprendre le cours normal de nos épisodes. Donc on parlera automobile, comme c'était prévu !

L : Oh j'ai hâte, j'ai hâte ! On se retrouve vite Charlie !

C : Avec joie Léa, ~~à tantôt~~ à la prochaine!**[JINGLE]**