**PROTÉGER SA VIE PRIVÉE ! - LE RIRE JAUNE (6 min 51)**

Protéger sa vie privée en 6 étapes

« Comment ça va YouTube ?

J’ai été contacté récemment par la CNIL et la MGEN

pour faire une vidéo humoristique afin d’aider les jeunes à mieux protéger leur vie privée sur internet.

J’ai accepté parce que j’ai trouvé la cause très louable et c’est là que…

Ils m’ont envoyé beaucoup de documents et de statistiques. C’est parti. »

# 1. Créer des mots de passe difficiles

« Alors là vous aller tous me dire merci Kevin, sans toi j’y aurais jamais pensé,

t’es le Mozart de la protection de données,

le Da Vinci du code de ma carte bancaire,

le Neper de mes logs,

t’as compris : login, log Néper parce que logarithme népérien.

Ah, ben, je tente le tout pour le tout, je ne perds rien, oh…

L’an dernier, une étude a montré que, sur 10 millions de mots de passe piratés, plus de la moitié faisaient partie des 25 suivants :

regardez, sérieusement : 123456, des suites logiques de chiffres, 6 fois de suite

le chiffre 6 puis 7 fois de suite le chiffre 7,

qwerty, google… Attends, mot de passe, les mecs ils ont vu ‘‘remplis mot de passe’’, ils ont rempli ‘’mot de passe’’, c’est les mêmes gars qui sont responsables de la blague ‘’trouver x, il est là’’.

T’imagines un hacker qui teste systématiquement ces 25 mots et qui connaît en plus ta date d’anniversaire, eh ! il pirate 80 % d’entre nous.

Pour éviter ça le plus possible, choisissez des mots de passe avec des symboles, des chiffres et des lettres, et essayez si possible d’avoir un mot de passe différent par site. »

(Il met une tasse et met du café puis il écrit ‘’par Sith’’)

(Thème musical connu de Star Wars)

# 2. Prévenir l’usurpation d’identité

« En appliquant le point 1, un hacker va avoir du mal à rentrer dans ton compte.

Par contre ça ne l’empêche pas de créer un clone identique à ton profil

et se faire passer pour toi afin d’arnaquer tes potes.

Je parle en connaissance de cause puisque je suis victime de ça tous les jours.

Depuis plusieurs mois, des centaines de faux comptes de youtubeurs sont apparus et se font passer pour nous

auprès de nos abonnés en vous faisant croire qu’il suffit d’appeler un numéro, surtaxé

évidemment, sinon ça serait pas drôle,

pour gagner un i phone. Certains y croient, se font arnaquer. Et le problème c’est qu’on est des personnages publics,

on peut vous avertir sur les réseaux et vous dire de signaler,

mais on ne peut pas tout contrôler alors que vous déjà, beaucoup plus.

La base c’est de ne rendre vos publications visibles qu’à vos contacts et votre liste d’amis visible qu’à vous-même.

Comme ça, un type qui veut t’usurper, il n’aura pas suffisamment de photos pour le faire

Et, s’il les a, c’est que quelqu’un parmi tes contacts te joue un sale tour…

C’est déjà plus facile à choper.

Retiens que 64 % des données piratées servent à usurper l’identité d’une personne

contre seulement 16 % pour les données bancaires.

Un hacker préfère avoir accès à un compte Facebook plutôt qu’à un compte courant.

Ah ! ben, il s’adapte à la crise, qu’est-ce que tu veux… »

# 3. Surveiller son référencement !

« Au lycée avec mes potes on tapait nos noms sur Google pour savoir qui était le plus ‘’famous’’.

Le moins connu devait une canette à tous les autres. Ah ! j’en ai perdu, de la thune.

C’est dommage qu’on n’y joue plus aujourd’hui, parce que…

Mais à l’âge adulte, se googliser régulièrement peut vous sauver un job.

35 % des recruteurs avouent avoir déjà écarté un candidat suite à des traces négatives retrouvées en ligne !

Imaginons que t’es soupçonné de trafic de drogue, mais que t’es innocent. J’ai dit imaginons… Ha ! on sait tous que t’es coupable.

Un article publie une liste de suspects, il y a ton nom dedans et, finalement, t’es blanchi.

Next thing you know !

5 ans plus tard, lors d’un entretien, ton recruteur, qu’on va appeler M. Léon,

tombe sur ton blase dans l’article.

Du coup, comme lui aussi il aime la Marie-Jeanne, il t’embauche direct

et là il te fait : ‘‘Il y a un moyen que tu m’en refiles un peu gratos ?’’

Sauf que toi t’as rien à voir là-dedans ; et quand il comprend que tout ça c’est du mytho,

là il se vénère, là il te vire.

Sauf que si tu étais abonné à tonton Kevin avant, tu aurais su qu’en France il existe le droit d’opposition

et de déréférencement plus lien. Tu peux demander à un site d’anonymiser le contenu et au moteur de recherche de supprimer

le rapport entre ton blase et le contenu gênant. »

**3.1 Droit d’opposition**

En France, vous pouvez directement demander à un site qui diffuse des informations sur vous de dépublier ou d’anonymiser le contenu.

**3.2 Droit de déréférencement**

Vous pouvez même demander au moteur de recherche de supprimer le lien entre votre nom, prénom, et un contenu gênant. Le contenu continue à exister sur internet mais, si un recruteur tape votre nom et prénom, il ne tombera pas sur ce contenu…

« Quelqu’un qui tape ton nom ne tombera pas dessus facilement, et tu te serais pas fait virer par ton boss le camé…Léon, eh, eh ! »

# 4. Distinguer sphère privée de sphère professionnelle !

« Supposons, par miracle cette fois-ci, que tu n’aies pas été viré, que tu travailles toujours dans cette entreprise ’’employé modèle’’,

et que durant tes week-ends tu pratiques ta passion qui est de faire des sketches sur YouTube.

Tu peux pas partager le dimanche soir sur ton mur une vidéo où tu fais ça :…

puis le lendemain matin demander à M. Léon une augmentation.

Ben oui, il va te répondre : ‘’Quand je te demandais de te bouger le cul, j’entendais pas ça !’’

Mélanger vie privée et vie professionnelle peut nuire à ton image si l’écart est trop grand entre ce que tu es en vrai et

le mytho que tu veux être au bureau.

Exemple : avoir vos collègues en amis sur FB.

Bien sûr, ça dépend du niveau de tolérance de l’entreprise aussi. Ha !

Moi par exemple, tous mes cadreurs travaillent à poil, donc, euh…

Perso mes opinions politiques, religieuses et photos compromettantes de soirées

c’est uniquement sur WhatsApp entre potes. Après c’est toi qui vois si tu t’en fous ou pas, si tu penses que ça va te porter préjudice ou pas.

Mais si t’as besoin de débattre publiquement d’un sujet polémique, penses peut-être à utiliser un pseudo. C’est une suggestion !

Ça t’offrira plus de liberté, comme traiter ton YouTubeur préféré de gros lard sans

que ce dernier puisse te retrouver pour te manger ! »

# 5. Prudence sur ce que vous diffusez !

« Ça nous est tous déjà arrivé de twitter un truc débile sans avoir réfléchi,

de regretter et de supprimer direct après.

Mais le problème c’est que sur internet il y a celui qu’on appelle (chanson) ‘’Peter le screener’’,

‘’Oui, c’est Peter le screener, il passe ses journées sur les réseaux

à la quête d’une lémique-po,

dès qu’il a trouvé,

commande 3 enclenché,

te voici désormais piégé à tous jamais ! Peter !’’

#kevinchanteur

On a tous un peu de Peter le screener en nous mais certains sont beaucoup plus Peter que d’autres, et là

ça devient dangereux : imagine t’es une meuf, tu matches avec un mec.

Vous faites un skype, ça devient érotique, le mec se déshabille et tu joues le jeu,

next thing you know.

En fait il t’a enregistrée et menace de diffuser la vidéo à tout ton entourage si tu ne fais pas ce qu’il veut.

**5.1 Chantage à la webcam**

Ça s’appelle le chantage à la webcam

et c’est le nouveau fléau du XXIe siècle.

Alors, écoutez-moi bien, là je vais vous donner des conseils, vous les trouverez pas sur le site de la CNIL, nulle part…

Quand t’envoies une vidéo, une photo érotique

sur Snap, ce que tu veux… : pas de moitié du visage !

Pas de tatouage ! Pas de bracelet !

Pas de grain de beauté visible sur le bas du ventre machin, RIEN

qui puisse trahir ton identité.

Si c’est une D#CK PIC,

prends toujours la photo d’en-dessous, tu verras que ça paraîtra plus… Hein, quoi ?

On sort complètement du cadre de la vidéo, désolé… »

# 6. Effacez vos données de navigation !

« Ce n’est pas parce que tu vas sur un site de cul

uniquement en navigation privée

qu’il ne faut jamais nettoyer l’historique de ta navigation publique !

Ça ne fait que te rendre plus suspect !

Quand tu lis un livre, le livre il ne conserve rien sur toi,

**6.1 #cookie**

alors qu’une page web, si.

J’ai un pote, il s’est fait cramer comme ça.

Il cherchait une bague de fiançailles pour sa copine.

Et là, bim ! Elle rentre dans la pièce. Lui, normal, il ferme tous les onglets,

sauf que le soir même sa meuf utilise l’ordi.

Et là forcément sur Facebook elle voit les suggestions de pub à côté !

Elle comprend ce que mon pote cherchait :

‘’acheter bague fiançailles…en faux diamant pas cher’’.

Ah, il s’est fait plaquer direct !

Bref, pour conclure : peu importe

notre âge, on forme ensemble la première génération qui doit

apprendre à vivre avec les réseaux sociaux

et il est vital de faire ça tout en protégeant notre vie privée

et nos informations personnelles.

Mais j’espère que cette vidéo à but préventif permettra de réduire un peu les risques.

Merci à la CNIL et la MGEN pour toutes les informations qu’ils m’ont données.

J’ai beaucoup aimé faire cette vidéo.

Et pour ceux qui veulent en apprendre plus sur comment réagir,

que faire quand on est victime d’usurpation d’identité et

de chantage à la webcam, etc., je vous ai mis plein de liens dans la description.

Sur ce, je vous dis à très bientôt pour une nouvelle vidéo.

Abonnez-vous !

Signalez les fakes !

Écrit per Kevin Tran

Réalisé par Raphaël Sartoris

Merci à @raphael\_liot

Produit par IDZ Prod

Musique par Gary Fico et Julien Comblat