Souriez, vous êtes en sécurité

Nina Cercy

@NLaPalice

1991
PGP

2017
Que Choisir

2017 : pas brillant

La bonne sécu ?

Celle que tu utilises.

modèle de menace, quoi qu'est-ce ?

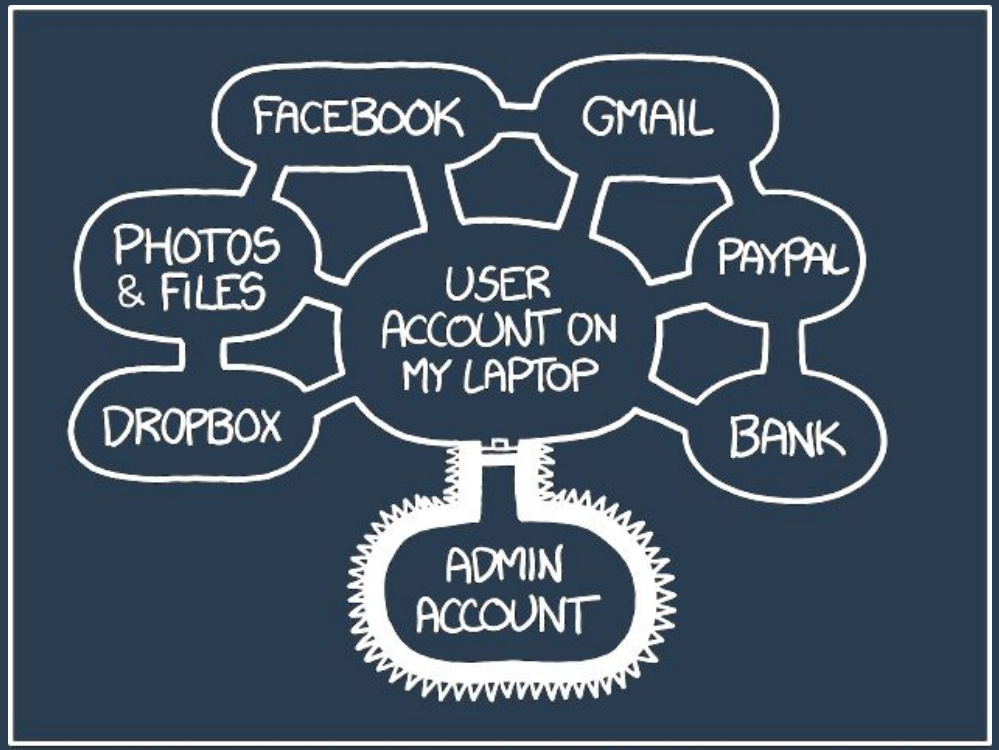
1. identifier ce qu'on veut protéger
2. identifier les risques qui pèsent sur nous
3. identifier les mesures pour s'en prémunir

Approche par les RISQUES
Approche par les CONSÉQUENCES

Pas de recette magique

Et Google, c’est le mal ?

objectif(s) Lune



IF SOMEONE STEALS MY LAPTOP WHILE I'M LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY MONEY, AND IMPERSONATE ME TO MY FRIENDS,

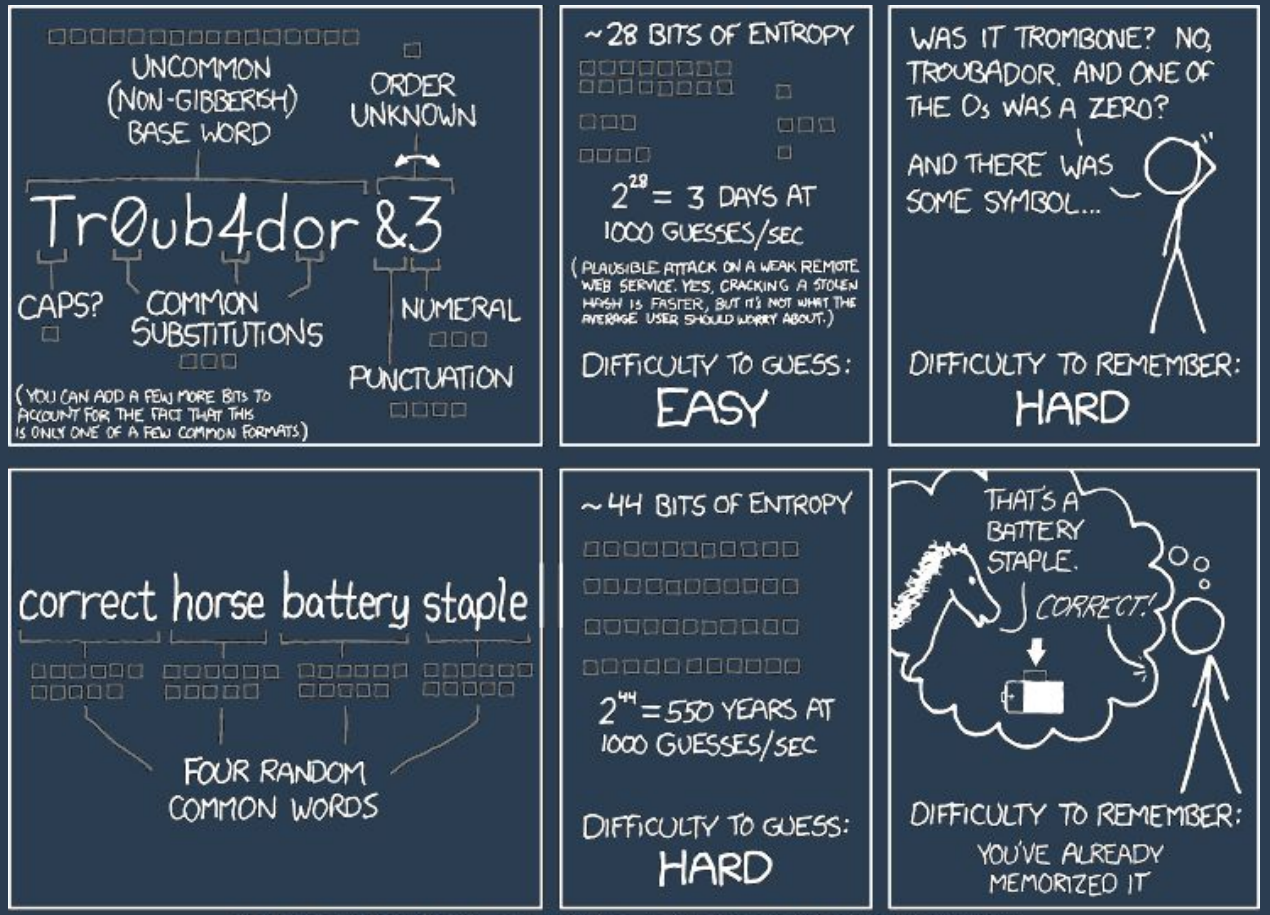
BUT AT LEAST THEY CAN'T INSTALL DRIVERS WITHOUT MY PERMISSION.

1. identifier ce qu’on veut protéger

2. identifier les risques qui pèsent sur nous

3. identifier les mesures pour s’en prémunir

“ jaipatontemps”



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Kévin “welcome to my life” Dupuis Morizeau

Sphère de l’intimité. Syndrome du “j’ai rien à cacher”

Soit lié à des risques personnels, comme son copain qui est jaloux, soit potentielle victime d’attaques de masse (phishing, spam, leak de bases de données avec son mot de passe).

Ca dépend. Peut-être que le copain de Kévin est très jaloux. Que ses parents sont des tyrans. Qu’il va se faire vider son compte en banque.

Ce qu’il faut bien comprendre, c’est que Kévin s’en foutra tant qu’il n’aura pas été confronté à la réalisation du risque. On ne peut lui donner que les conseils de base, facilement applicables. Oui, Kévin va rester sous Windows. Antispam, gestionnaire de mots de passe, 2FA.


Kévin
17h59

Suite et fin.

CERCY, Nina <nina.cercy@hec.edu> Jul 26

to

Bonjour,

Manifestement je n'ai pas été assez claire en arrêtant de répondre aux mails, en changeant de numéro de téléphone et en bloquant votre Facebook : je ne veux plus entendre parler de vous.

Ça fait déjà quelques mois que je n'ai plus envie de discuter, et j'ai découvert il y a deux mois qu'une partie de notre correspondance avait "mystérieusement" disparu. Exclusivement les mails les plus explicites que vous m'aviez envoyé. Ils manquaient aussi dans la correspondance que vous m'avez envoyé ensuite à ma demande. Je suis absolument furieuse, et nous étions les deux seuls à être au courant de cette conversation donc... Je ne pourrai jamais le prouver mais je n'ai aucun doute.

Au prochain message, je porte plainte pour harcèlement.

Michelle “*Hasta siempre!*” Yang, la journaliste

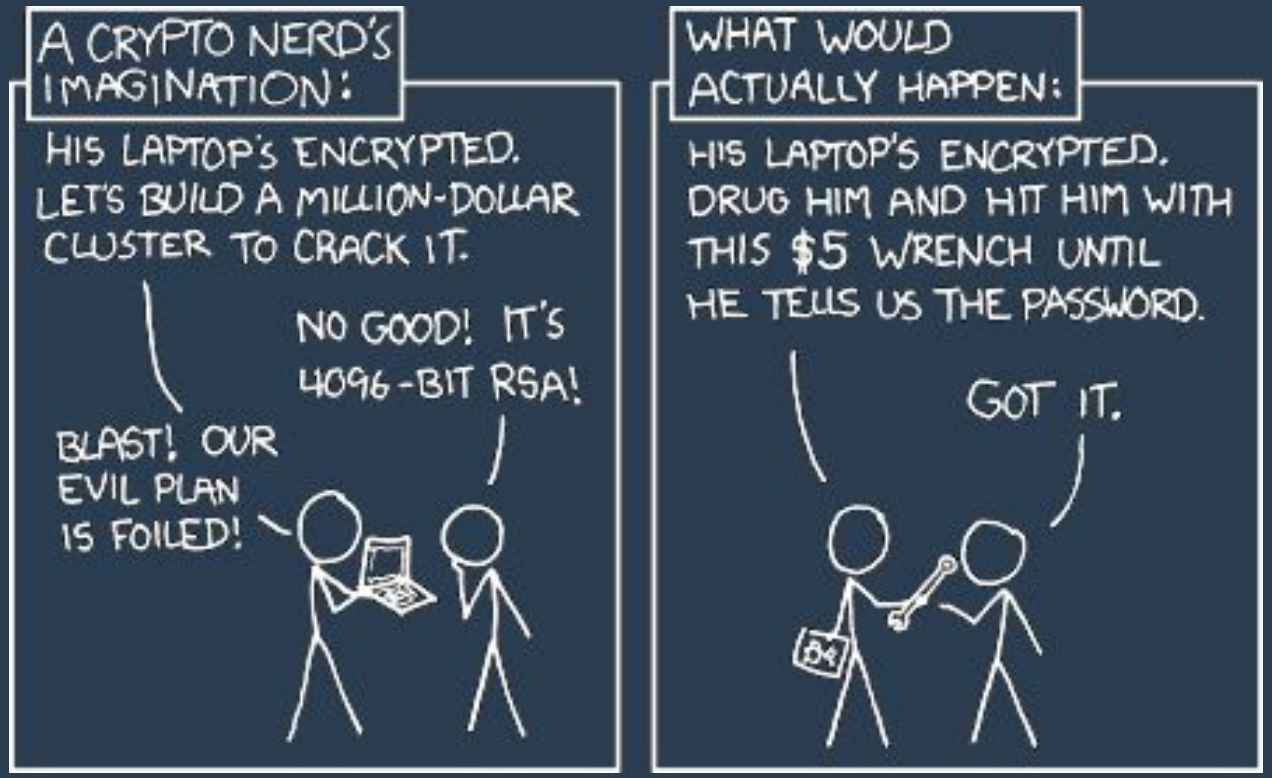
Données potentiellement décrédibilisantes, comportement sur internet, localisation, données sur lesquelles elle travaille, identité de ses sources...

Les gens sur lesquels elle détient des informations, l’Etat, renseignements généraux, militant.e.s qui ne l’aiment pas… Attaques physiques ou à distance.

Gravissimes : sources en danger, travail journalistique perdu, assignation à résidence, attentat...

Obligée de doublement se protéger : outils d’anonymat sur Internet, Secure Drop, mails chiffrés, TOR & Tails, mais également backups, chiffrés eux aussi. Souveraineté numérique essentielle. Double facteur d’authentification.

la (vraie) force brute



Sélim “l’homme pressé” de Tatol

Données essentiellement professionnelles car poste à responsabilité : carnet d’adresses, fichier clients, contrats avec des clauses de non divulgation, stratégie marketing CRUCIALE !!!

Contraintes réglementaires (coucou la GDPR !), concurrents prêts à tout pour mettre la main sur le plan marketing digital disruptif et ubérisant de Sélim

Conséquences désastreuses pour l’image de l’entreprise, potentielles grosses amendes…

Données centralisées, synchronisées, pas trop de mots de passe différents, effacement à distance, privilégier les outils connus et la collaboration facilitée


shadow IT

Patricia, la jeune pousse

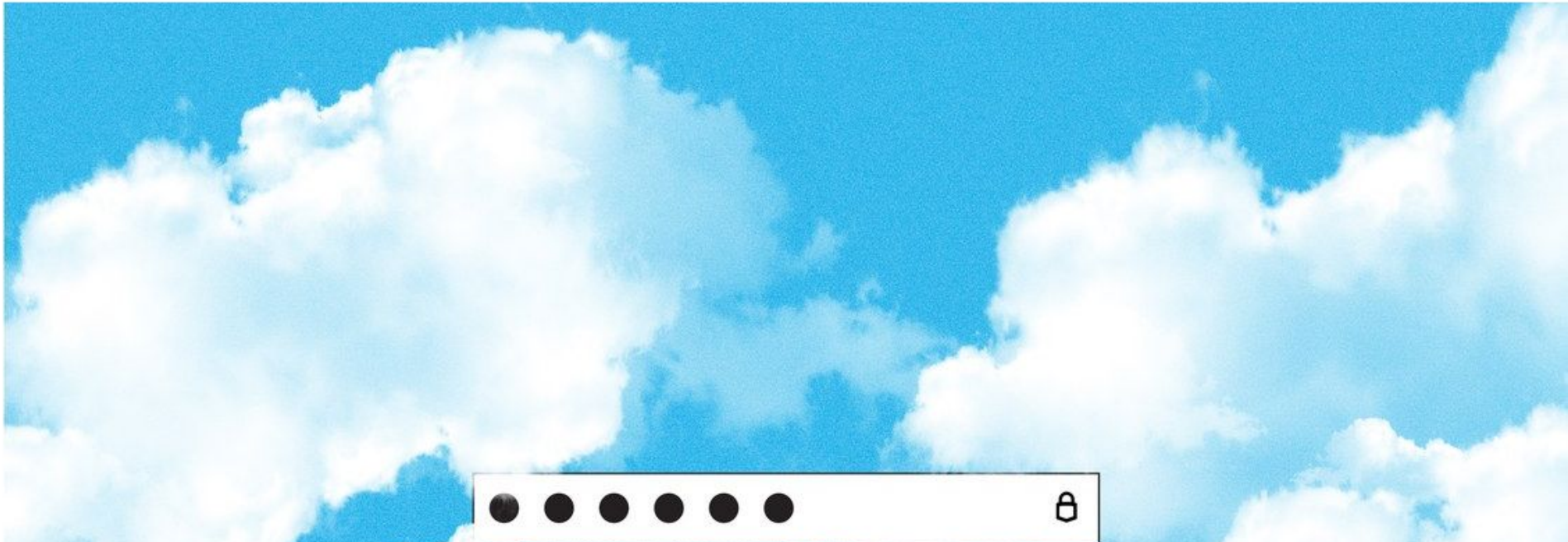
Etudes de marché prometteuses, fichiers internes, comparatifs, business plan

Peur de se faire piquer ses idées, elle a lu les meilleures pratiques sécurité.
Besoin de ne pas perdre ses documents, sauvegarde régulière, accès facile et rapide, pas d'interruption de service

Différence entre les risques perçus et les risques réels.

Faisons dans la demi-mesure : un petit Nextcloud server-side encrypted sur Dropbox ?

‘I FORGOT MY PIN’: AN EPIC TALE OF LOSING $30,000 IN BITCOIN



aeris @aeris22 · Feb 3

Un GG à @NLaPalice qui est la 1ère a réussir à shunter (presque) toutes mes sécurités et donc me fait offrir des croissants à @MyCozyCloud

Translate from French

2 8

aeris @aeris22 · Feb 3

Donc, mon nouveau modèle de menace passe à « ta collègue à 3m de toi qui veut des croissants gratos demain » :D @NLaPalice @MyCozyCloud

Translate from French

3 2

aeris @aeris22 · Feb 3

Au final, elle aura
- trouver comment changer de bépo à qwerty
- galérer à trouver mon client mail
[…]
@NLaPalice @MyCozyCloud

Translate from French

1 1

aeris @aeris22 · Feb 3

- Galérer 20min à rédiger un mail en qwerty
- Se rendre compte qu'elle ne peut pas l'envoyer
[…]
@NLaPalice @MyCozyCloud

Translate from French

2 1

aeris @aeris22 · 3 févr.

- Utiliser mon navigateur pour se connecter au webmail
- Se rendre compte qu'il faut un mot de passe
[…]
@NLaPalice @MyCozyCloud

1 1

aeris @aeris22 · 3 févr.

- Pleurer
- Se rendre compte que mon compte LastPass est toujours connecté
- Utiliser LastPass pour se connecter
@NLaPalice @MyCozyCloud

3 1

aeris @aeris22 · 3 févr.

- Regalérer 20min pour retaper le mail
- L'envoyer
Bien joué, vraiment :)
@NLaPalice @MyCozyCloud

2 1

modèle de menace

individuel ou social ?