LA SECURITE NUMERIQUE

Pour TOUS

LES MOLIERES - LES CAFES DU SAMEDI - ATELIERS

Grégoire LANCELOT

Questions et affirmations de base

- Suis-je vraiment concerné(e) ?
  - Tout utilisateur(trice) d'un ordinateur (et autres terminaux numériques) et d'internet est concerné(e)
- Je n'ai rien à cacher
  - Vraiment ?
- Je ne suis pas parano
  - Ça n'est pas une protection
- J'ai confiance
  - Sur quoi repose-t-elle ?

Qu’est-ce qu’une donnée à caractère personnel ?

DEFINITION DE LA CNIL (Commission Nationale de l’Informatique et des Libertés)

C’est toute information relative à une personne physique susceptible d’être identifiée, directement ou indirectement.

Par exemple : un nom, une photo, une empreinte, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de sécurité sociale, un matricule interne, une adresse IP, un identifiant de connexion informatique, un enregistrement vocal, etc.

Peu importe que ces informations soient confidentielles ou publiques.

A noter : pour que ces données ne soient plus considérées comme personnelles, elles doivent être rendues anonymes de manière à rendre impossible toute identification de la personne concernée : noms masqués, visages floutés, etc.

Attention : s’il est possible par recoupement de plusieurs informations (âge, sexe, ville, diplôme, etc.) ou par l’utilisation de moyens techniques divers, d’identifier une personne, les données sont toujours considérées comme personnelles.

Règlement Général sur la Protection des Données (RGPD) (Europe)

- Adopté le 27 avril 2016 et entré en vigueur en 2018

https://www.cnil.fr/fr/reglement-europeen-protection-donnees

https://www.economie.gouv.fr/entreprises/obligations-donnees-personnelles-rgpd

- Il s'applique à toutes les entreprises et organisations qui traitent des données personnelles de citoyens de l'UE, quelle que soit leur localisation géographique.
- Il établit de nouvelles obligations pour les entreprises et organisations en matière de protection des données, notamment en ce qui concerne la notification des failles de sécurité, la transparence et les choix des personnes concernées.
- Il renforce les droits des personnes concernées en matière de protection de leurs données personnelles, notamment en leur donnant le droit de savoir si leurs données sont collectées, à qui elles sont communiquées et comment elles sont utilisées.
- Il impose des sanctions financières importantes aux entreprises et organisations qui ne respectent pas les règles édictées par le RGPD.

Quelques chiffres

- 3 minutes pour pirater un nouvel objet connecté
  1,1 million de victimes de fraude à la carte bancaire par an
  +83 % de smartphones infectés au 2e semestre 2016
  65 vols de données par seconde
  41 % : le taux de succès d'un ransomware
  201 jours pour découvrir une cyberattaque
  1,7 milliard de publicités fraudeuses en 2016
  140 attaques de phishing par heure
  Les particuliers deux fois plus infectés que les professionnels
  Une entreprise subit 29 cyberattaques par an

source : https://www.silicon.fr/hub/malwarebytes-hub/cybersecurite-les-10-chiffres-qui-font-peur

- 54 % des entreprises françaises attaquées en 2021
  +255 % d'attaques par ransomware
  50 000€, c'est le coût médian d'une cyberattaque
  Une perte moyenne de 27 % du chiffre d'affaires en France
  Seules 50 % des entreprises victimes portent plainte
  47 % des télétravailleurs se font piéger par un phishing
  35 % des attaques utilisent de nouvelles techniques
  82 % des employeurs inquiets quant au télétravail

source : https://www.stoik.io/cybersecurite/chiffres-cles

Les questions à se poser ?

- Que souhaitez-vous protéger ?
  - Données bancaires
  - Documents et photos
  - Contacts
  - Opinions, activités ...
- De qui souhaitez-vous protéger ces données ?
  - Entreprises
  - Etats
  - Activistes criminels
- Jusqu'où êtes-vous prêt(e) à aller pour les protéger ?
  - Changement d'habitudes
  - Etapes supplémentaires
  - Solutions payantes

Des menaces multiples

- Vos données valent de l'or
- Aucune sécurité n'est absolue
- Les pirates s'organisent en entreprises avec de gros moyens
- La grande majorité des piratages sont dus à de la négligence et la méconnaissance
- Le hameçonnage (phishing) vise les particuliers comme les entreprises
  - https://www.cnil.fr/fr/cnil-direct/question/le-phishing-cest-quoi

Quelques exemples de dangers

- Cold boot attack
  - https://blog.f-secure.com/fr/attaques-cold-boot/
- Des données effacées peuvent être récupérées
- Un mot de passe Windows ne protège rien
- Failles Zero Day
- Piratage des laboratoires et hopitaux
- Rançongiciels (ransomewares)
- Surveillance en ligne

Bonnes pratiques générales

- Réduire la surface d’attaque avec le chiffrement
- Utiliser des mots de passe forts et uniques
- Gardez vos systèmes et logiciels à jour
- Utiliser des câbles de sécurité pour attacher vos appareils en déplacement
- Ne pas céder à la psychose
- Mais rester toujours vigilant
- La surenchère est mauvaise conseillère !
- Eviter les portes blindées sur clôtures en bois

Messagerie

- Je protège les données de mes correspondants
- J'utilise le CCI
- Si possible j'utilise des adresses email différentes en fonction des activités
- Je n'ouvre aucune pièce jointe si l'origine du mail est douteuse
- J'évite de transférer des PJ
- Je contrôle les adresses des expéditeurs
- Je contrôle les liens avant de cliquer
- Je signale les tentatives de hameçonnage (voir site de la CNIL)

MOT DE PASSE

- Ne JAMAIS utiliser deux fois le même mot de passe pour deux applications différentes
- Toujours utiliser des mots de passe longs (15-20 caractères) et complexes, exemple type « pass phrase », ou générés aléatoirement par un outil dédié
- Utilisez un coffre fort local à mots de passe type KeePass
- Rester méfiant vis à vis des gestionnaires de mot de passe dans le cloud (LastPass)
- Ne jamais utiliser d'informations personnelles dans un mot de passe, ni de mots trop identifiables
- Ne jamais donner son mot de passe, encore moins si on vous le demande
- Utiliser si possible une authentification à deux facteurs

Stockage et données

- Disposer d’une sauvegarde hors ligne si les données sont en ligne
- Eviter de revendre des disques durs et clés usb
- Formatage bas niveau / données aléatoires et chiffrement
- Diversifier les moyens de stockage (cloud, local, auto-hébergement, archivage optique ...)
- Il existe des logiciels (comme Eraser) spéciaux pour supprimer les données de manière sécurisée

Logiciel et système

- La gratuité n’existe pas
- Privilégier l’open source / logiciel libre
- Ne pas confondre gratuit et libre
- Si envisageable financièrement, consulter les solutions alternatives payantes
- Mettez à jour vos systèmes et logiciels
- Utilisez des logiciels de nettoyage simples et efficaces comme bleachbit
- Toujours configurer les options de confidentialité

Réseau domestique

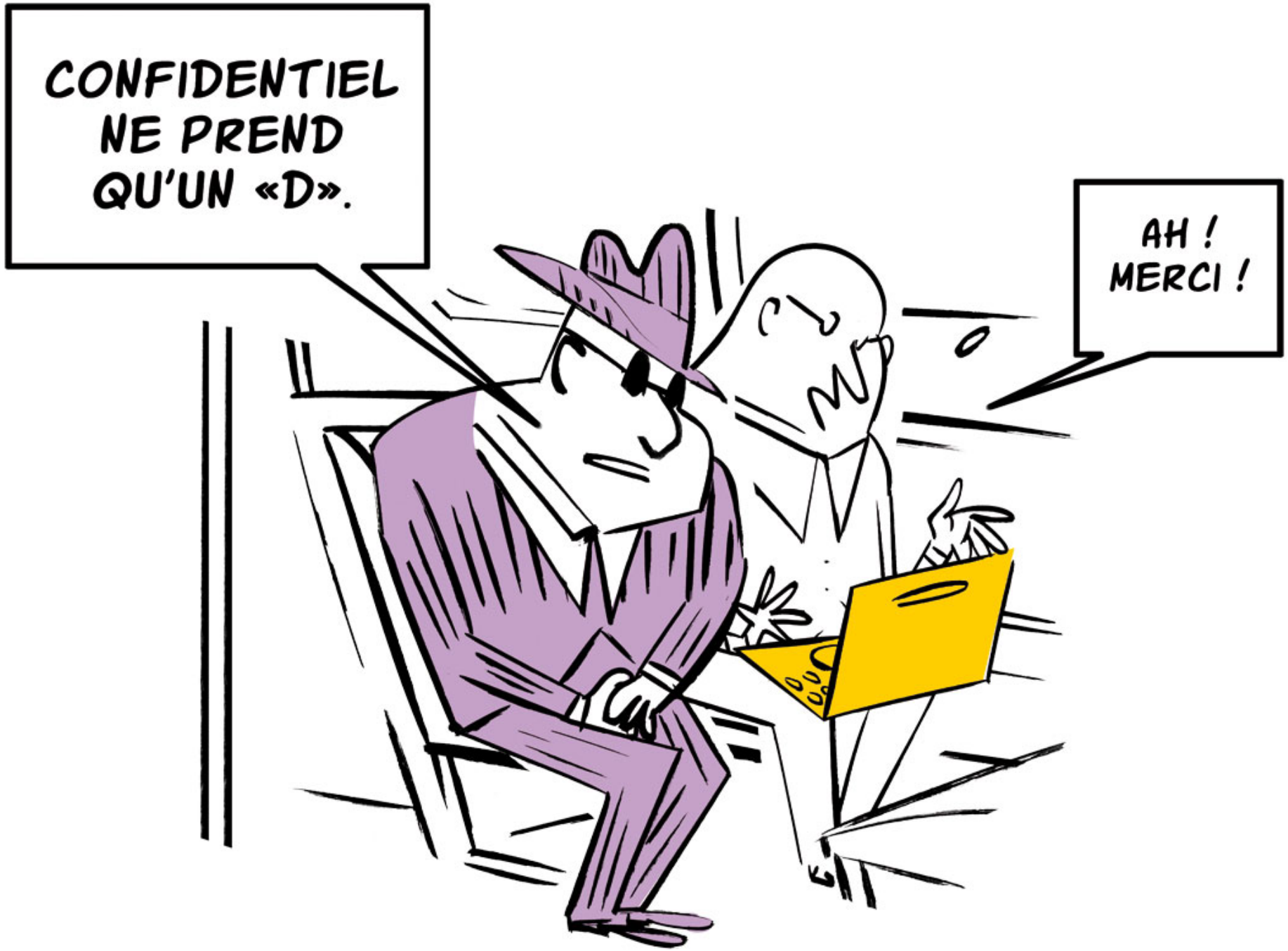
- Utiliser un pare-feu
- Utiliser un VPN
- Utiliser toujours une sécurité WIFI de type WPA2/3
- Utiliser le mot de passe WIFI le plus long possible et le changer de temps en temps
- Changer le mot de passe admin, le réseau et l'adresse de la box

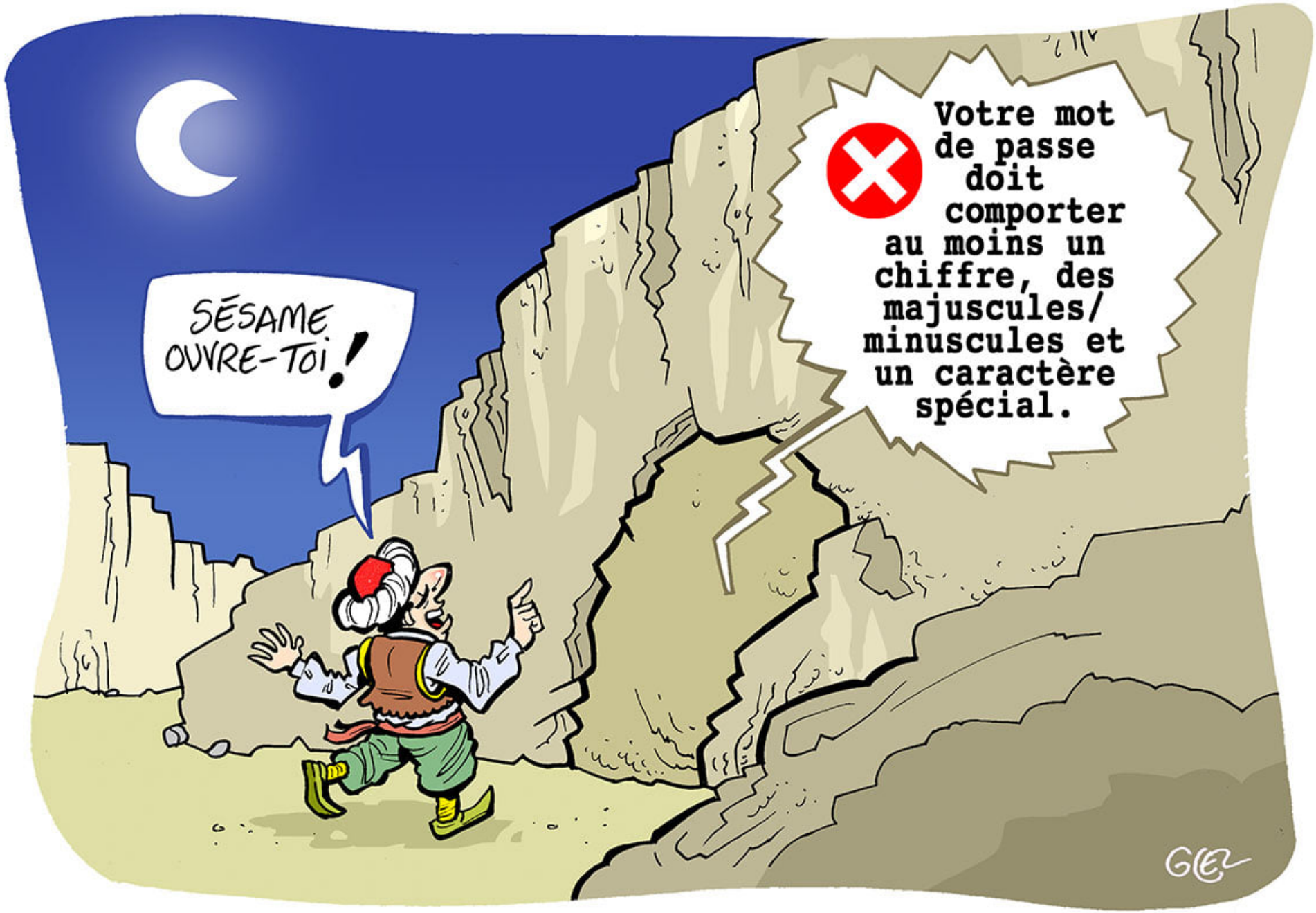
Navigation web

- Qu’est-ce qu’un cookie ?
- Attention aux trackers !
- Ne jamais renseigner de données bancaires ou personnelles sur un site non sécurisé (http sans le ‘s’) et de manière générale, ne pas visiter les sites web non HTTPS
- Vider régulièrement l’historique et les cookies ou utiliser des sessions privées
- Refuser systématiquement les cookies
- Etudier les solutions payantes et open source
- Vous avez des droits sur vos données récoltées

Smartphone

- Chiffrer le téléphone et la carte SD
- A minima code pin (pas 0000 ni 1234) pour la carte sim et un différent pour le téléphone
- Protéger les applications sensibles
- Ne pas utiliser d'applications non contrôlées par le magasin officiel
- Même WhatsApp s'est fait pirater (https://www.presse-citron.net/whatsapp-sest-fait-pirater-votre-numero-est-il-sur-le-dark-web/)
- Solutions SMS alternatives comme Signal, Wire ...
- Maximiser la confidentialité sur les réseaux sociaux
- Un VPN et un pare-feu sont également utilisables sur un smarphone


CONFIDENTIEL NE PREND QU'UN «D».
AH ! MERCI !


SÉSAME OUVRE-TOI !
Votre mot de passe doit comporter au moins un chiffre, des majuscules/ minuscules et un caractère spécial.

Merci

Questions

"Si vous pensez que l'éducation coûte cher, esssayez donc l'ignorance"

Abraham Lincoln