Se protéger avec de bons mots de passe

Vincent Mazenod, expert à la CRSSI DR7, CNRS

F11 plein écran, touche ←, ↑, →, ↓ pour naviguer

Pourquoi un mot de passe ?

Alors que je n'ai rien à cacher?

Vraiment rien?

- vous êtes donc prêt à publier sur le web
  - toute vos correspondances?
    - mails pro?
    - mails perso?
    - facebook?
    - meetic?
  - tous les fichiers sur lesquels vous travaillez?
  - vos déplacements sur google maps?
  - tout votre historique de recherche google?
  - votre déclaration de revenu?
- "Je n'ai rien à cacher" par Julien Vaubourg
- "Si, vous avez quelque chose à cacher" par @Numendil
- "Why privacy matters" by Glenn Greenwald

Ok! peut-être n'ai-je pas envie que tout cela se sache mais ...

Qui cela peut il bien intéresser?

- professionnellement (au moins) vous faites partie d'un tout
  - vos informations peuvent être réutilisées pour en atteindre d'autres
    - ingénierie sociale en vue d'une intrusion dans un système d'information

- une clé USB restée sur un poste fixe, un ordinateur portable égaré et ...
  - l'envie de rendre service
  - la simple curiosité
  - le challenge technique
  - l'appât du gain
- ... sont des moteurs qui poussent les autres à s'intéresser à **vos données** alors qu'**ils n'y ont pas été invités**

Le mot de passe ... une question d'hygiène

un mot de passe

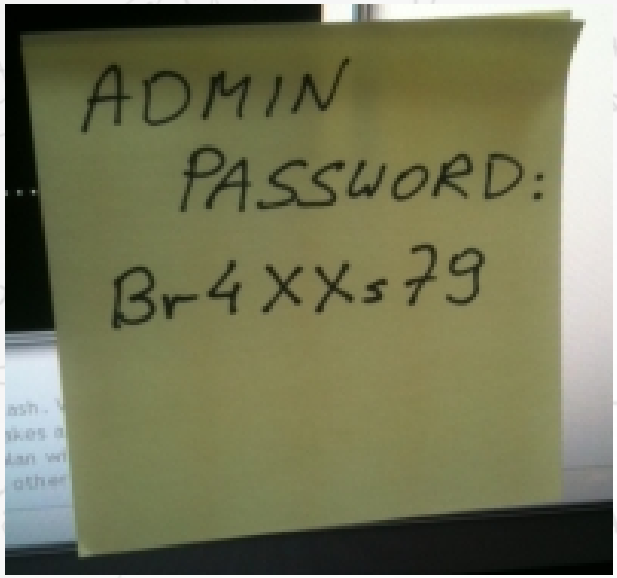
1. ça ne se prête pas
2. ça ne se laisse pas traîner à la vue de tous
3. ça ne s'utilise qu'une fois
4. si ça casse on remplace immédiatement
5. ça n'est jamais assez sophistiqué
6. pour être bien protégé mieux vaut choisir la bonne taille

Ca vous rappelle quelque chose?

1 - Ca ne se prête pas

2 - Ca ne se laisse pas à la vue tous

on détruit



- les post-it sur l'écran avec le mot de passe de l'appli de gestion
- les post-it sous le clavier avec le mot de passe de connexion
- l'impression papier du mail de réinitialisation de mot de passe, ou de confirmation d'inscription d'un site de e-commerce
- toutes les pages de dossiers faisant figurer un quelconque mot de passe
- les carnets d'adresses papier avec le code de CB, le digicode etc ...

on arrête de "retenir les mots de passe"

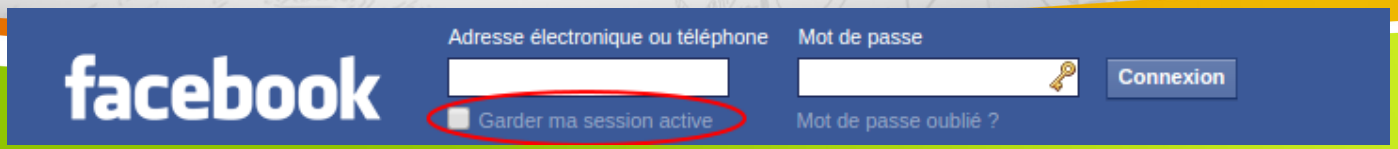
2 - Ca ne se laisse pas à la vue tous

- connaissez vous ce bouton?

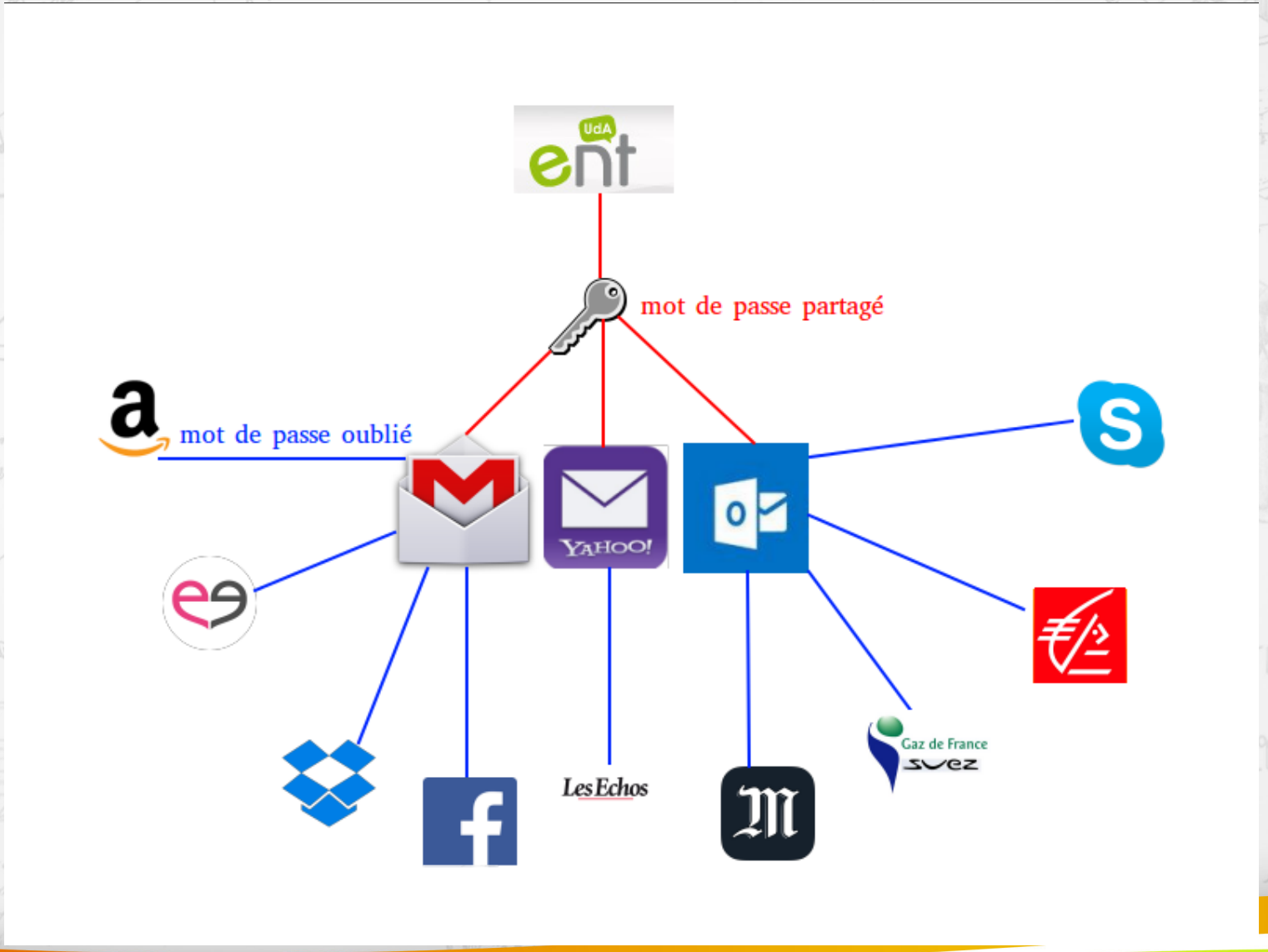
déconnexion

  - Quand vous
    - utilisez une machine qui n'est pas la vôtre
    - quand vous laissez votre machine sans surveillance
    - partez de votre bureau
    - avez fini de vous servir d'un service
  - **déconnectez vous**
    - ne pas le faire reviendrait à laisser le coffre fort en libre accès le jour des portes ouvertes de la banque

on arrête de cocher "se souvenir de moi"



3 - Ca ne s'utilise qu'une fois



4 - Si ça casse on remplace immédiatement

- Vous avez prêté votre mot de passe
- Votre mot de passe a été vu
- Vous avez utilisé votre mot de passe pour un autre service
- Vous pensez avoir été victime d'un piratage
- Le service que vous utilisez vous conseille de changer de mot de passe
  - Attention toutefois aux tentatives d'hameçonnage (phishing)
    - A minima vérifiez l'url de la page de changement de mot de passe
    - Ne renvoyer JAMAIS votre mot de passe en clair dans un mail ou un document en PJ
- **Vous avez un doute?**

Changez votre mot de passe

5 - Ca n'est jamais assez sophistiqué

Sachez qu'il ya le bon **et le mauvais mot de passe ...**

Le mauvais mot de passe

- c'est celui auquel tout le monde pense

Password Popularity – Top 20

Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542

Rank	Password	Number of Users with Password (absolute)
11	Nicole	17168
12	Daniel	16409
13	babygirl	16094
14	monkey	15294
15	Jessica	15162
16	Lovely	14950
17	michael	14898
18	Ashley	14329
19	654321	13984
20	Qwerty	13856

  - avec ces 20 mots de passe on pouvait pirater presque 40% des comptes de rockyou.com en 2009
  - imaginez ce que l'on peut faire avec ce bête fichier texte et quelques lignes de programmation
- **c'est celui qu'on retrouve en deux clics sur google ou facebook**
  - votre date de naissance
  - le nom de votre conjoint
  - le nom de vos enfants ...

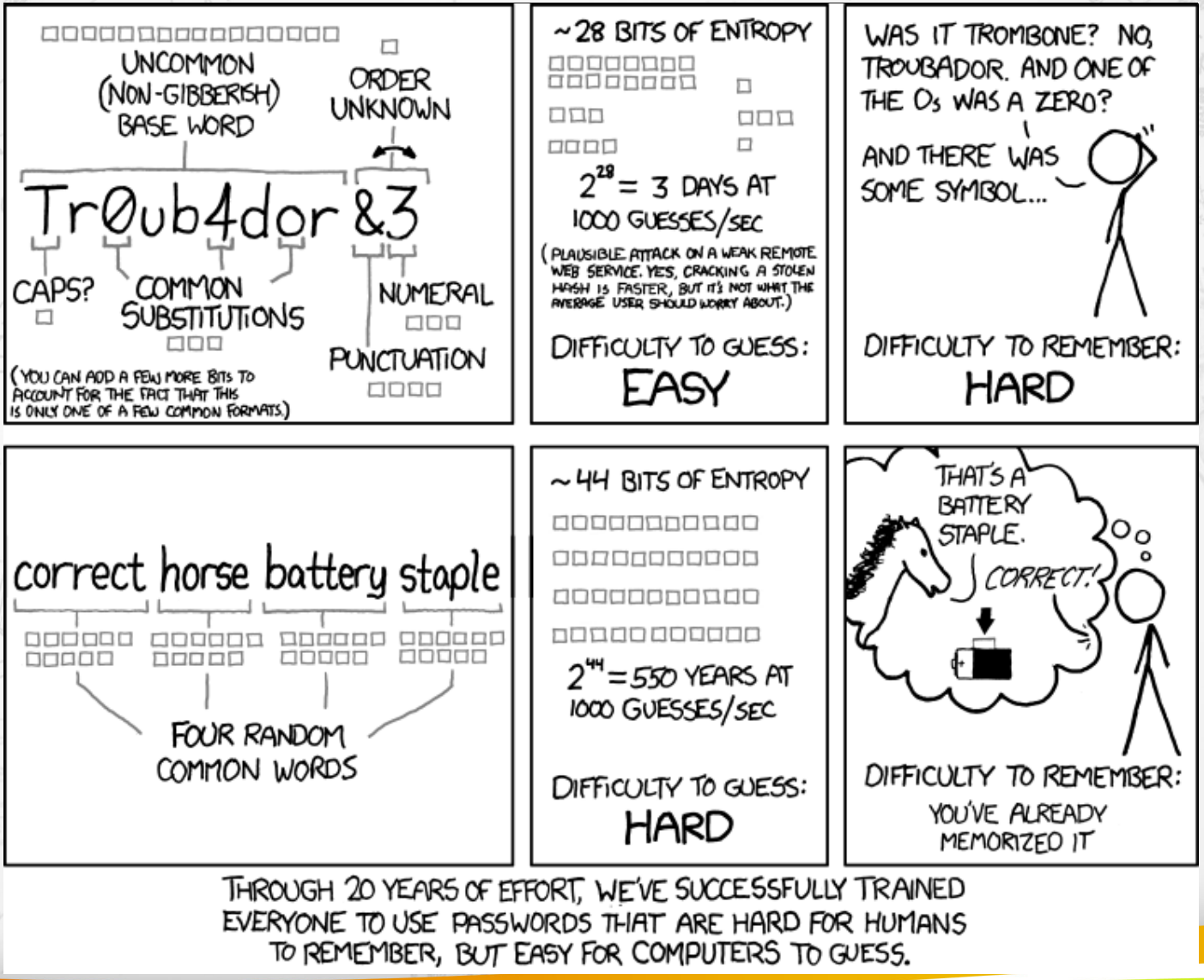
Le bon mot de passe

- doit être fort
  - pas devinable
    - pas dans le dictionnaire
  - doit contenir
    - plus de 8 caractères
      - règle d'hygiène n°6: pour être bien protégé mieux vaut choisir la bonne taille
  - doit utiliser au moins 3 des 4 ensembles de caractères
    - des majuscules
    - des minuscules
    - des caractères spéciaux
    - des chiffres
- vérifier la robustesse
  - Password checker de Microsoft
  - passwordmeter.com
  - et surtout http://mdp.u-clermont1.fr

La technique du leet speak

- le leet speak de l'anglais « elite speak » rend les mots incompréhensibles
  - Microsoft → M1CR0$0F7
  - ashley → 4$hL3y
  - newbie → noob → n00b
  - elite → leet → 1337
  - leet speak converter

La technique de la phrase de passe



La technique du mantra

ou comment s'améliorer en même temps que sa sécurité

- je dois me coucher avant minuit
  - vaaulitavant00
  - Sleep@before12
- je m'arrête de fumer
  - stop!la!clope!
  - Quit@smoking4ever
- je viens de me faire plaquer
  - loublier<3
  - Forgive@h3r

Votre objectif est atteint?

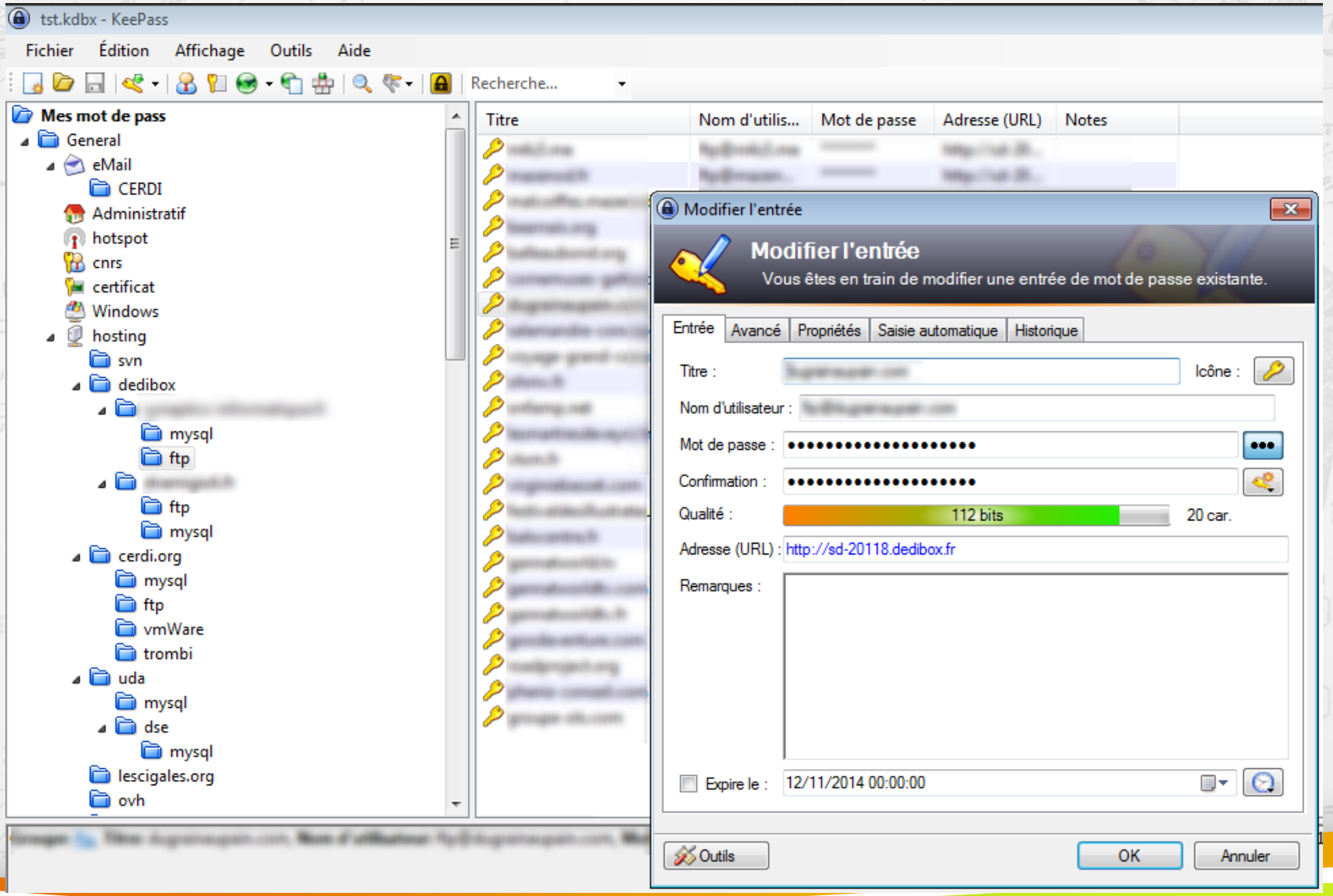
- **Vous pouvez changer de mot de passe et choisir un nouveau mantra**

La génération de mots de passe aléatoires

- strongpasswordgenerator.com
- newpasswordgenerator.com
  - RJ+hEv5S6Ky@z?nCW_gctN4M
    - est **très robuste**
    - est **très difficile à mémoriser**

Comment retenir plusieurs dizaines voire centaines de mots de passe plus ou moins complexe?

KeePass


tst.kdbx - KeePass
Fichier
Édition
Affichage
Outils
Aide
Recherche...
Mes mot de pass
General
eMail
CERDI
Administratif
hotspot
cnrs
certificat
Windows
hosting
svn
dedibox
mysql
ftp
ftp
mysql
cerdi.org
mysql
ftp
vmWare
trombi
uda
mysql
dse
mysql
lescigales.org
ovh
Titre
Nom d'utilis...
Mot de passe
Adresse (URL)
Notes
Modifier l'entrée
Modifier l'entrée
Vous êtes en train de modifier une entrée de mot de passe existante.
Entrée
Avancé
Propriétés
Saisie automatique
Historique
Titre :
Icône :
Nom d'utilisateur :
Mot de passe :
Confirmation :
Qualité :
112 bits
20 car.
Adresse (URL) :
http://sd-20118.dedibox.fr
Remarques :
Expire le :
12/11/2014 00:00:00
Outils
OK
Annuler

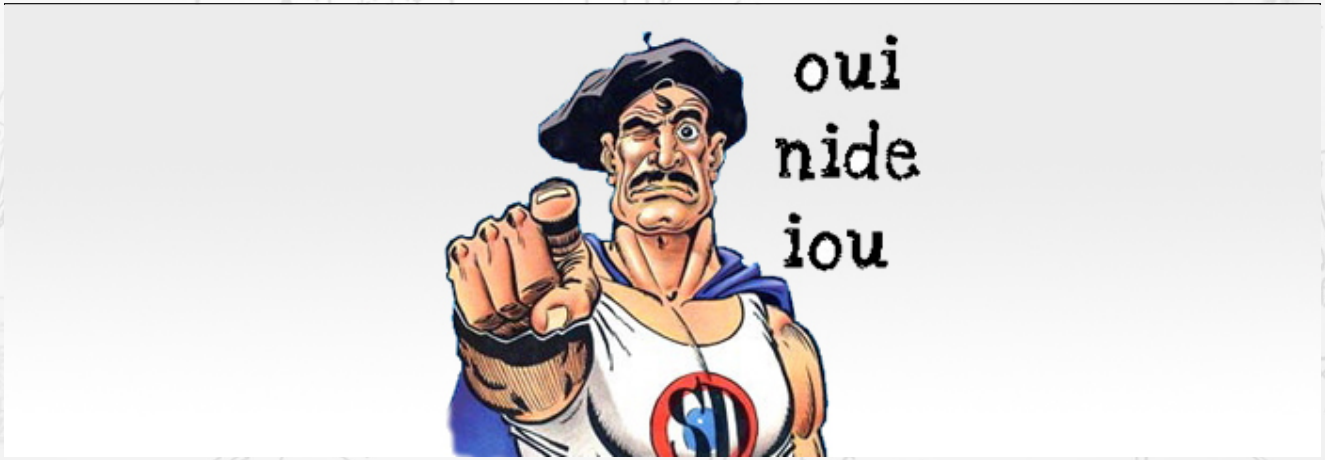
KeePass

- Le meilleur logiciel de gestion de mot de passe
  - centralise tous vos mots de passe dans un seul fichier chiffré
  - installable sur tous vos périphériques
    - existe sous Windows, Mas OS X, linux, iOS, Android, Palm OS
    - existe en version portable (il peut s'exécuter à partir d'une simple clé USB)
- il est aussi
  - libre et gratuit
  - capable de tester la robustesse de vos mots de passe
  - capable de générer des mots de passe
  - certifié par l'ANSSI
  - téléchargeable ici
  - ... et bien plus encore
  - **n'oubliez pas le bon mot de passe que vous aurez mis à votre catalogue de mot de passe ;)**

N'oubliez pas que

- nous détenons tous des informations sensibles
- la confidentialité de nos données est souvent liée à celle des autres
- être attentif au choix et à la gestion de ses mots de passe est à la portée de tous
  - et vous pouvez commencer dés maintenant
- il existe des outils pour vous faciliter la vie
- ... et que la plus grosse faille de sécurité
  - se trouve bien souvent entre la chaise et le clavier

Soyez acteur de la sécurité de l'information [inscription au MOOC jusqu'au 30 novembre 2014]



Merci de votre attention!

Des questions?