COPÉA
Accueillir
Expérimenter
Entreprendre

Association nationale des coopératives d'activités et d'entrepreneurs

Comment éviter les pièges du web ?

Ou pourquoi ne pas faire confiance à azerty ...

Atelier Rencontre des CAE
Vendredi 20 Septembre 2019
Le lazaret à Sète

Florent Le Saout
florent.lesaout@astrolabe.coop
https://www.astrolabe.coop

Présentation

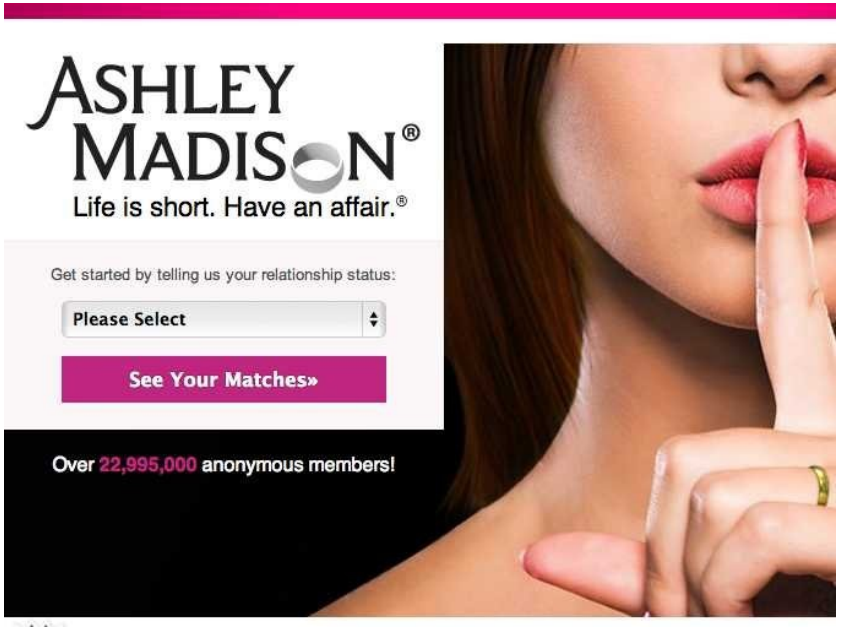
- Astrolabe CAE
- Votre hôte
- La présentation
- Et vous ?

Plan

- Contexte
- Risques
- Les sites web
- Les emails
- Les mots de passe
- Les solutions
- Mise en pratique

Contexte

- Base de données divulguées sur internet
  - Ashley Madison (33M)
  - AdultFriendFinder (442M)
  - Yahoo (500M)
  - Twitter
- Coût estimé des pertes
- Dégâts familiaux etc...



Risques

- Usurpation d’identité
  - Faible degré => réseaux sociaux
  - Moyen => soutirer de l’argent à des proches
  - Important => création de faux papiers d’identité
- Aspect psychologique avec préjudice moral
  - Biométrie
    - Reconnaissance faciale
    - Reconnaissance d’empreintes
    - Mieux vaut une bonne gestion de mots de passe

Les sites web

- Man In the middle
  - Hotspot
  - Malware
- Faux sites
  - Noms très proches ou qui induisent en erreur
- Gestion des cookies (vie privée) : RGPD

Les solutions

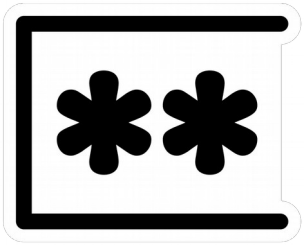
- Un peu de bon sens
  - Garder son esprit critique
- https et certificat
- Enregistrer les adresses (pas de moteur de recherche)
- Avoir un système et des logiciels à jour

Les emails

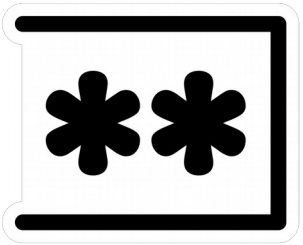
- Faux emails sites officiels
  - Banque
  - Service public
- Site de menace contre rançon
  - Demande bitcoin sinon révélation d’informations
- Gain loterie
- Fishing

Les solutions

- Ne jamais cliquer sur les liens des emails
  - Un site officiel ne demandera jamais de cliquer sur un lien
- Aller sur Hoaxbuster :
  - https://www.hoaxbuster.com/



Mots de passe



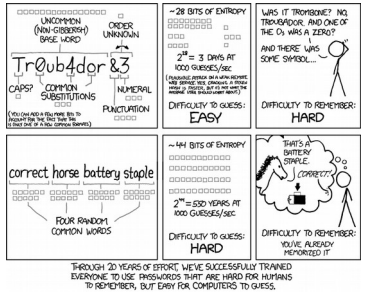
- Trop courts
- Trop simples
- Le même pour tous les sites
- Mot de passe email de secours non sécurisé ou pas assez
- Question secrète basique (social engineering)
- Hameçonnage/Fishing avec collecte du mot de passe
- Keylogger, Trojan, les failles
- ';--have i been pwned?

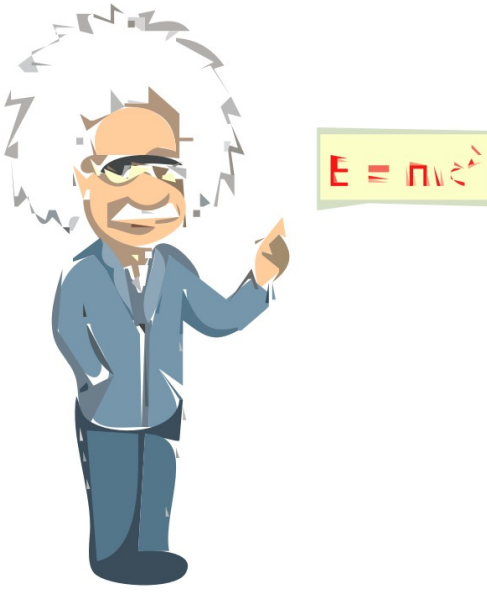
Dangers

- Cas de mots de passe trop simples
  - Attaque par dictionnaire (Base de données) => N mots de passe/secondes
- Cas de mots de passe trop courts
  - Attaque par force brute (Génération aléatoire de mot de passe) => N mots de passe/secondes
- Cas de tous les mots de passe similaires
  - Base de donnée cassée => réutilisation sur les services les plus courants

Les solutions : Théorie

- Se fabriquer un vrai mot de passe
  - Les mots de passe les plus utilisés
  - Temps pour craquer les mots de passe en fonction de la complexité
  - Appli de test de mots de passe
- Diversité, multiplicité, complexité
  - Mettre des mots de passe différent pour chaque service
  - Noyer l'info dans d'autres infos





Les solutions : Outils

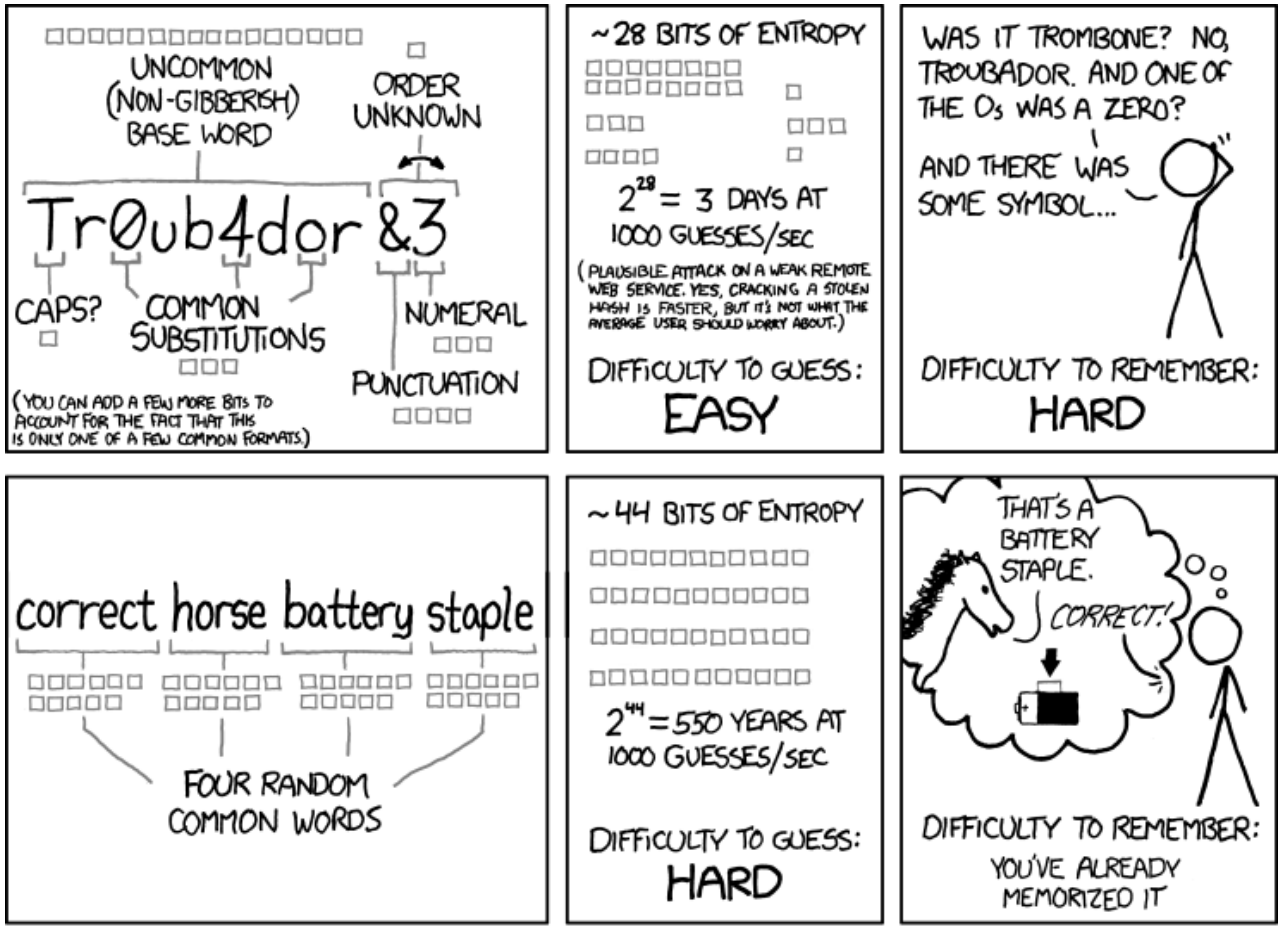
- Bonnes pratiques
  - Limiter le stockage des mots de passe dans les navigateurs
  - Utiliser le mode navigation privée
  - Gestionnaire de mots de passe

- Détection des risques
  - https://haveibeenpwned.com

Les solutions : outils

- Stockage et génération de mots de passe :
  - Keepass2
    - Stockage local ou en ligne
  - KeepassX

Conclusion


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS:
EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER:
HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS:
HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT
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.

Questions & Discussion

Les solutions : mise en pratique