

Comment épater votre entourage avec des te...

par Michel Kartner - <http://www.leblogduhacker.fr/comment-epater-votre-entourage-avec-techniques-de-hacking/>

Lien vers l'article en ligne :

<http://www.leblogduhacker.fr/comment-epater-votre-entourage-avec-techniques-de-hacking/>

Comment épater votre entourage avec des techniques de hacking

Vous n'avez **pas** besoin de faire carrière dans la sécurité informatique, ni besoin d'apprendre 36 langages de



programmation pour **épater** votre entourage.

Tout le monde ne connaît pas tout sur l'informatique (et à vrai dire, personne ne connaît tout).

Je vous ai donc sélectionné 5 techniques de hacking pour épater vos proches, elles peuvent s'avérer drôles, surprenantes, effrayantes.

Certains me diront « euh c'est pas du hacking » je leur répondrai :

Résultats de recherche

hacker

Définitions Web

Un hacker est une personne qui montre une passion pour la compréhension du fonctionnement intime des systèmes, ordinateurs et réseaux informatiques en particulier.

N'allez tout de même pas croire que vous allez **pirater** ou nuire avec ces techniques, il s'agit plutôt de trucs et astuces pour tout public. Ils ne sont plus non plus très récents.

1. Comment faire un dossier impossible à supprimer

Appuyez sur *Windows* et *R* en même temps

- Tapez *cmd.exe*
- Tapez dans l'invite de commande : *cd C:\Le_Chemin_De_Votre_Choix* (vous allez créer le dossier dans ce chemin)
- Tapez : *md con* (*md* signifie *make directory* – créer un dossier) n'oubliez pas le « \ » de fin.

Essayez de supprimer le dossier crée 😊

Comment épater votre entourage avec des te...

par Michel Kartner - <http://www.leblogduhacker.fr/comment-epater-votre-entourage-avec-techniques-de-hacking/>

Vous ne pourrez pas non plus le renommer.

Pour le supprimer, il doit être **vide**, et il vous faut taper :

```
rd con\ à la place de md con\
```

Note: Non, ça ne veut pas dire que *Windows* détecte que vous voulez écrire un gros mot, c'est simplement un nom réservé signifiant « console ».

D'autres mots sont réservés comme *aux*, *nul*, *lpt1*, *lpt2*, *lpt3* jusqu'à *lpt9*. Si vraiment ça vous intéresse vous avez la liste ici : <http://support.microsoft.com/kb/74496/fr-fr>.

2. Comment tester votre antivirus

Si votre antivirus ne détecte pas ce qui va suivre, je ne peux que vous conseiller de le **changer**.

L'*EICAR* (*European Institute for Computer Antivirus Research*) a prévu une façon standard de **tester** un antivirus (initialement prévu pour les développeurs d'antivirus).

Comme ils le disent sur [leur page](#), il s'agit de tester **rapidement** et **facilement** un antivirus. Utiliser un **vrai** virus pour cela serait comme mettre le feu à la poubelle du bureau pour voir si le détecteur de fumée fonctionne.

Voici donc la signature de test, vous pouvez ouvrir un nouveau fichier texte et copier/coller ce code. Essayez ensuite de scanner votre fichier pour tester votre antivirus.

```
X5O!P%@AP[4PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Vous pouvez également l'enregistrer sous le format ".bat" et double cliquer dessus pour voir si votre antivirus lance une alerte de ce type :

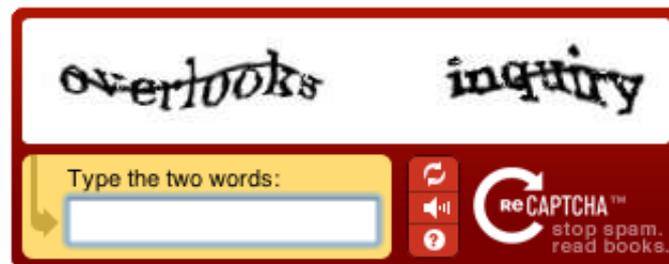


3. Gagnez du temps avec les captchas

Vous connaissez sûrement très bien les **captchas**, vous empêchant de télécharger votre série préférée en un clic.

[reCaptcha](#) est un service proposé par Google permettant de **stopper** le spam sur Internet, mais pas uniquement.

En effet, le système de captcha fait du **deux en un**, un mot sera validé par le système, tandis que l'autre servira à améliorer le processus de numérisation de livres, là où échouent les systèmes de [reconnaissance optique de caractères](#) (OCR).



Du coup, un mot sur les deux n'est **pas nécessaire** pour valider le test. Et souvent ce mot est reconnaissable, il est plus **clair** que l'autre.

Dans l'image ci-dessus je suppose donc qu'il s'agirait de "overlooks" qui serait **optionnel** et qui peut donc être **remplacé** par n'importe quelle lettre (Notez qu'il faut tout de même écrire quelque chose suivi d'un espace, suivi du deuxième mot).

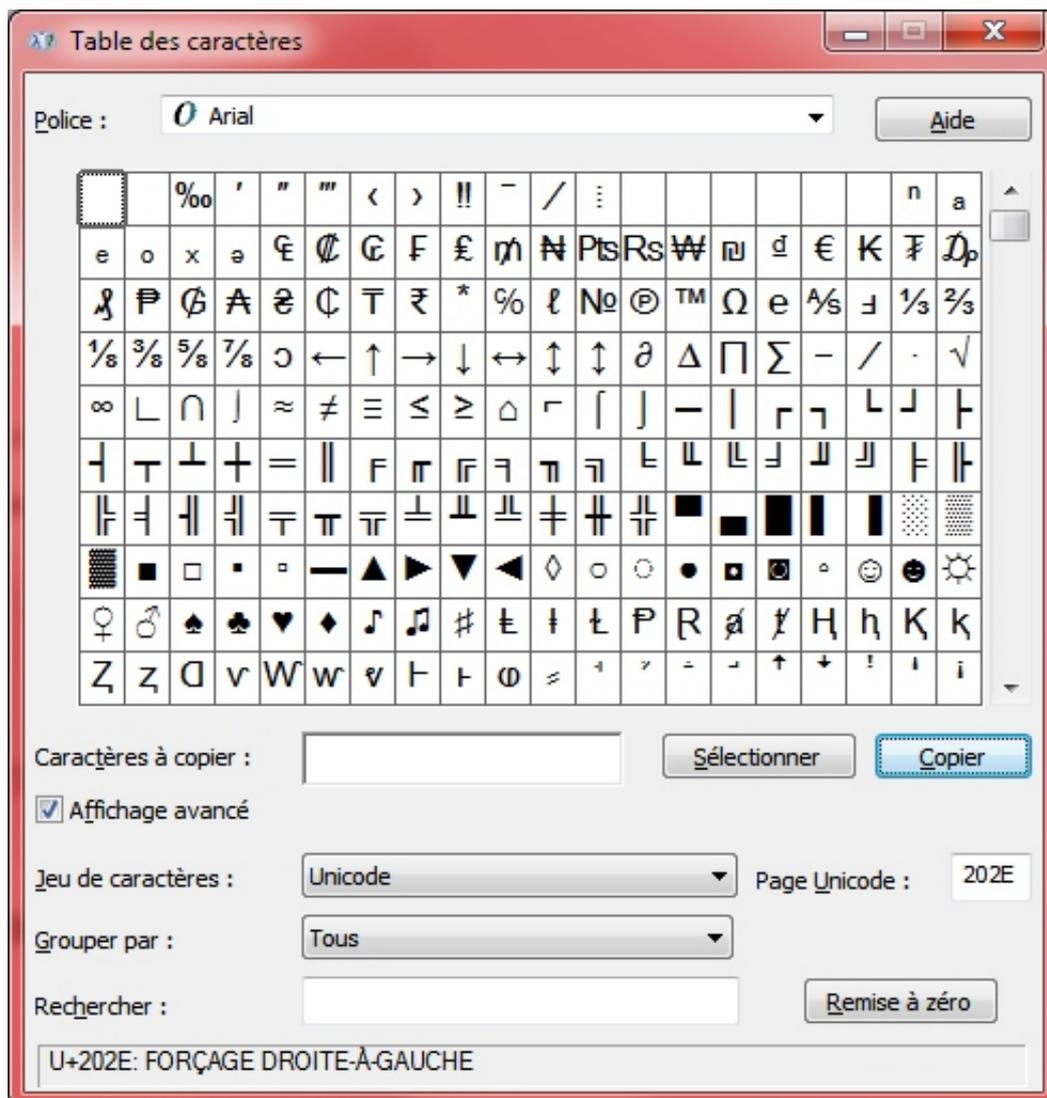
4. Changer l'extension .exe en .jpg

Une des techniques de hacking souvent demandées par les hackers malveillants qui cherchent à faire exécuter leur programme en faisant croire à la victime qu'elle clique sur une **image**.

Sachez que oui, c'est possible de littéralement changer le nom de **.exe** à **.jpg** sans passer par quelque chose comme **image.jpg.exe**.

Il s'agit d'utiliser un caractère spécial, le forçage droite-à-gauche permettant donc d'écrire de la droite vers la gauche.

Pour le trouver, appuyez sur *Windows* et *R* en même temps, tapez "**charmapp.exe**".



Dans la fenêtre qui s'affiche, tapez "202E" pour la **Page Unicode**, cliquez ensuite sur **Sélectionner** et puis sur **Copier**.

Rendez vous vers votre fichier, renommez-le, tapez quelque chose comme "unnom[CTRL+V]gpj.exe". À la place de [CTRL+V] vous copiez le caractère que vous venez de copier.

Bonus : Dans la même lignée des astuces avec les caractères, il existe des caractères Unicode qui sont placés au **dessus** (ou en dessous) des autres, ou simplement à des endroits non communs.

En 2009, il y a donc eu un mini buzz avec [Zalgo](#), permettant de copier/coller des textes un peu spéciaux dans les forums, dans les commentaires ou même en guise de pseudo.

Assez enfantin, je dois l'admettre.

5. Trois mots de passe pour se connecter à Facebook

Saviez-vous que vous pouvez vous connecter à votre compte *Facebook* avec **3 mots de passe différents** ?

Facebook autorise effectivement plusieurs façon de se connecter, vous pouvez tester par vous-même.

1. Se connecter avec son mot de passe normal

Jusqu'à là rien d'anormal, imaginons que le mot de passe de notre compte soit **motDePasse**. Ce que je ne vous conseille pas !

C'est le cas par défaut, nous pouvons nous connecter comme d'habitude.

2. Votre mot de passe avec la casse renversée

La casse ? Vous en avez sûrement entendu parler avec "la sensibilité à la casse" indiquant que le système gère la **différence** entre majuscules et minuscules.

Facebook autorise donc la casse renversée, vous pouvez transformer les majuscules en minuscules et inversement.

Du coup, pour notre exemple, on pourra se connecter avec : **MOTdEpASSE**.

3. Votre mot de passe original avec la première lettre en majuscule

Tout est dit, dans notre cas il s'agira de **MotDePasse**.

Ce n'est pas une faille de sécurité mais une **fonctionnalité** offerte par *Facebook* depuis longtemps.

C'est par exemple du à des raisons **mobiles**, certains mobiles mettent automatiquement la première lettre en majuscule.

Saviez-vous que pour le nom d'utilisateur il existe **aussi** 3 manières de se connecter ?

1. L'adresse e-mail

2. Le nom d'utilisateur (si défini)

3. Le numéro de téléphone (si défini)

On a donc 9 façons de se connecter à *Facebook*.

Plus de tutoriels inédits sur le Hacking sur le site web [Le Blog Du Hacker](#)