Endroits où placer votre lien piégé

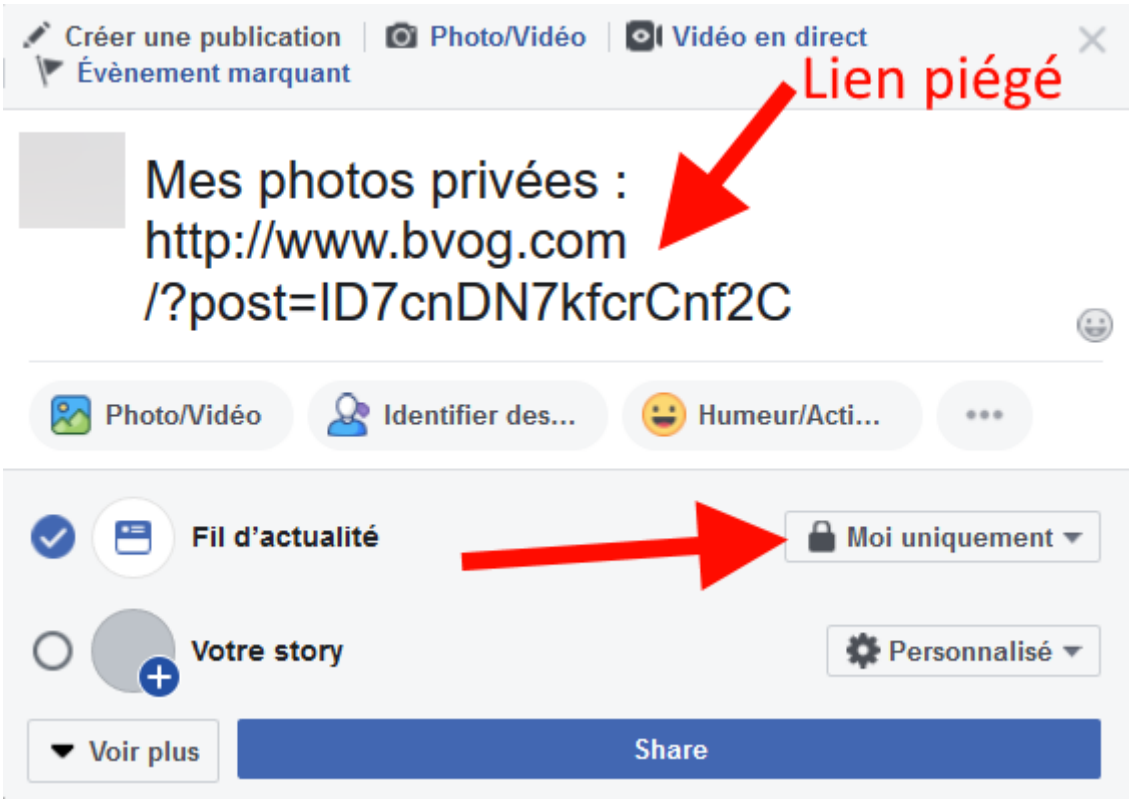
Ce document fait référence à la vidéo du cours sur le hacking éthique qui traite des pièges à placer sur vos systèmes pour être alerté(e) si jamais un pirate venait à entrer dans votre système.

La liste se veut bien entendu non exhaustive, mais cela peut vous donner quelques idées de démarrage rapide.

1. Sur les comptes des réseaux sociaux, en mode privé

Le fait de placer un lien sur un profil de votre compte en ligne visible par vous uniquement permettra de recevoir une alerte si une personne ayant accès à votre compte clique sur votre lien.

Sur Facebook par exemple, vous pouvez publier votre lien de la façon suivante :



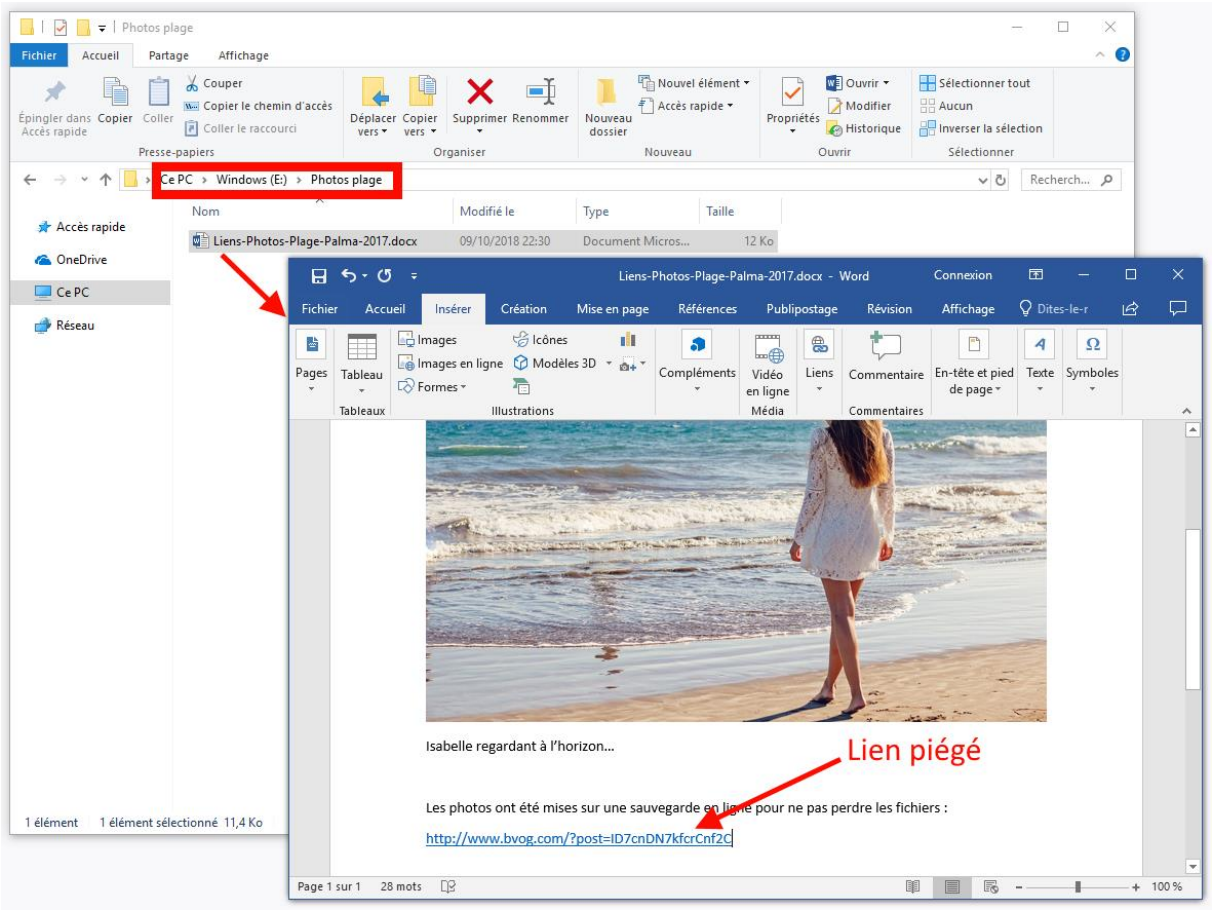
2. Sur votre ordinateur, dans des documents ou dossiers sensibles

L'idée générale est d'être réaliste dans vos pièges, et de faire en sorte qu'un intrus clique, sans pour autant lui laisser penser qu'il s'agit d'un piège…

Pour cela, vous pouvez tenter de faire un dossier « Privé » dans le dossier « Documents », voir sur le Bureau. Mais si vous pensez que cela ne convient pas, n'hésitez pas à essayer l'un des mots-clés parmi les suivants :

- Important
- Photos plage
- Mot de passe
- Mon amour
- Fiches de paie
- Etc

Vous pouvez ensuite y placer un fichier Word ou PDF menant (soi-disant) vers le contenu en question :



3. Sur un site web, à des endroits sensibles

Si vous administrez un site web et/ou qu'un espace sécurisé en ligne, n'hésitez pas à y placer votre ou vos liens pièges de façon à ce qu'une personne ayant accès à vos comptes puisse cliquer assez facilement sur le ou les liens.

Vous pouvez par exemple vous baser sur l'exemple précédent, en créant des dossiers pièges à la racine du site.

Ou alors, les placer dans des pages « brouillon » ou non publiées que seul un administrateur (en l'occurrence vous ou un pirate de votre compte puisse voir).

Vous aurez également l'avantage d'avoir vous-même des liens, et de pouvoir créer des redirections sans avoir besoin de raccourcisseurs d'URL.

4. Sur une clé USB, un disque dur ou un smartphone

Quoi de mieux pour savoir si on utilise vos périphériques en votre absence ?

N'hésitez pas à vous baser sur les techniques précédentes ou à les adapter selon vos divers périphériques.

Sur smartphone, vous pouvez bénéficier d'un e-mail piégé également, ou alors utiliser des SMS. À ce propos, vous pouvez demander à un complice (ou utiliser des services en ligne) pour vous envoyer un SMS avec le lien piégé :

5. Par e-mail, ou tchat en ligne avec un complice

N'hésitez pas à partager le lien avec un complice (qui ne cliquera pas sur le lien ensuite…). Les pirates voudront sans doute se mêler de votre vie privée, et observer vos conversations, alors c'est l'endroit idéal pour placer des pièges ! N'hésitez pas à être inventif en plaçant les liens dans des documents envoyés. Mais attention à ne pas non plus surcharger les conversations de liens.

Vous pouvez demander à votre complice de vous envoyer votre lien piégé pour plus de réalisme, ou complètement inventer une discussion avec un faux profil que vous aurez vous-même créé.

La méthode est vraiment très souple et s'adapte à toutes les situations.

Astuces générales

Il est évident qu'il existe des possibilités infinies et que les exemples donnés peuvent paraitre trop simples ou non adaptés. Il convient donc à chacun d'adapter cela à sa situation et à ses systèmes.

Voici d'autres pistes et idées :

- Utiliser des liens différents pour chaque piège (de façon à savoir qu'est-ce qui a été cliqué).
- Tester régulièrement vos liens vous-même
- Masquer vos liens avec des raccourcisseurs d'URL
- Essayez les QR code pour masquer les liens
- Associez divers liens à diverses adresses e-mail différentes…au cas où…

NOTE importante sur les faux positifs

Il est tout à fait possible que vos liens soient « cliqués » par des robots de Facebook, Google, Microsoft ou d'autres. Cela vous prouve non seulement qu'ils suivent (espionnent ?) les liens publiés, mais surtout que vous n'avez pas à vous inquiéter pour le clic en question.

Malheureusement il est impossible d'éviter cela, parfois vous aurez même plusieurs alertes pour une même personne ou un même outil qui clique plusieurs fois.

Restez vigilant(e) et méfiant(e), mais prenez le temps d'analyser le message reçu.

Et ensuite ? comment savoir qui a concrètement cliqué ?

Vous pouvez utiliser des sites de géolocalisation comme : https://www.iplocation.net/

Vous pouvez déposer plainte si besoin, en ayant la preuve avec vous.

Vous pouvez bloquer l'adresse IP (pare-feu ou règles de filtrage sur votre site)

Vous pouvez envoyer un autre lien piège à une personne que vous soupçonnez, si l'adresse IP est la même, vous avez une très forte probabilité qu'il s'agisse de cette personne !

Michel du site Le Blog du Hacker.

PS : vous pouvez cliquer sur tous les liens de ce document, il n'y a aucun piège, promis ! 😉