MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

7 conseils pour lutter contre le piratage informatique

La lutte contre le piratage informatique est l'affaire de toutes et de tous. Voici des règles simples pour éviter de se faire pirater.

1

Ne téléchargez pas de programmes ou modules (*plug-ins*) depuis des sites non-officiels.
Ils peuvent contenir des logiciels espions invisibles qui vous volent vos mots de passe (*stealers*) et peuvent bloquer votre ordinateur ou votre téléphone.

2

Utilisez un anti-virus à jour et ne le désactivez jamais.
Un anti-virus permet de détecter une grande partie des menaces, s'il est bien à jour. Ne désactivez jamais un anti-virus ; les logiciels malveillants invitent à le désactiver pour pouvoir s'installer.

3

Méfiez-vous des messages inattendus.
Par exemple, ceux qui viennent d'un interlocuteur inhabituel. Au moindre doute, ne les ouvrez pas, ne cliquez sur aucun lien et n'ouvrez aucune pièce jointe : ces messages peuvent vous piéger pour dérober des informations confidentielles ou installer un virus.

4

N'utilisez pas le même mot de passe partout.
Privilégiez des mots de passe différents sur chaque service en ligne afin d'éviter les piratages en cascade.

5

Imaginez des mots de passe robustes et activez les authentifications renforcées quand c'est possible.
Utiliser des mots de passe forts (12 caractères, minuscules, majuscules et caractères spéciaux) qui ne disent rien sur vous. Évitez vos noms et prénoms, vos dates de naissance, soyez créatifs !

6

Appliquez les mises à jour de sécurité sur tous vos appareils (PC, tablettes, téléphones, etc.) dès qu'elles vous sont proposées.
Vous corrigez ainsi les failles de sécurité qui pourraient être utilisées par des pirates pour vous voler vos données et mots de passe.

7

N'enregistrez pas vos mots de passe dans un ordinateur partagé et pensez à vous déconnecter en partant.
Sinon vos mots de passe et vos sessions seront aussi partagés.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

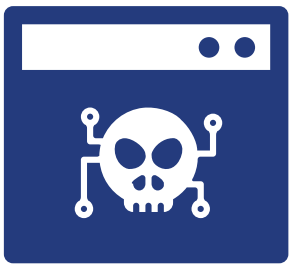
PIRATAGE DE COMPTES ENT ET DE LOGICIELS DE VIE SCOLAIRE

Mise en garde face aux virus «**dérobeurs**» (*stealers*)

En partenariat avec
POLICE NATIONALE
le ministère de l'Éducation nationale et de la Jeunesse
et le ministère de la Justice

Les établissements scolaires ont connu une vague importante de fausses alertes à la bombe, diffusées via les Espaces Numériques de Travail (ENT) ou des applications de gestion de vie scolaire. Si ces faits ont faibli depuis l'interpellation de plusieurs individus, **des comptes d'élèves, dont les identifiants ont été volés, sont encore utilisés pour poster des messages sur ces applications à leur insu**.

Lors des investigations, plusieurs logiciels malveillants de type *stealer* ont été retrouvés sur des ordinateurs personnels d'élèves.



QU'EST-CE QU'UN *STEALER* ?

Les virus informatiques de type *stealer* sont spécialisés dans le vol d'identifiants (mots de passe…), de portefeuilles de cryptomonnaies, de cookies de session et autres données stockées notamment dans les navigateurs Internet.
Une fois exfiltrées, ces données sont utilisées par les cybercriminels à des fins frauduleuses ou malveillantes.

MÉTHODES D'INFECTION

À titre d'illustration, dans le cadre du dossier des fausses alertes à la bombe, les *stealers* ont été introduits intentionnellement dans des logiciels contrefaits non validés par les éditeurs originels. Le virus a plus précisément été diffusé via des liens postés sur différentes plates-formes grand public comme, par exemple, les réseaux sociaux (messages d'hameçonnage ou *phishing*). Certains liens étaient même parfois proposés dans les premiers résultats des moteurs de recherche. Les utilisateurs ont notamment été invités à installer des extensions de jeux vidéo qui leur promettaient d'améliorer leurs performances. Parfois, les messages ont même indiqué de désactiver l'antivirus avant de télécharger et d'installer le programme ou l'extension infectée, ce qui a permis au *stealer* d'éviter d'être détecté. Le scénario d'infection a donc ciblé, comme c'est souvent le cas, une catégorie d'internautes en exploitant leur intérêt. Dans notre cas, les jeunes et les jeux.

LE RISQUE DES MOTS DE PASSE STOCKÉS DANS LES NAVIGATEURS

Il est très simple d'enregistrer dans son navigateur Internet ses mots de passe, ses adresses de messagerie, ses coordonnées de cartes bancaires, etc.
Ils présentent cependant des risques importants face aux *stealers* qui cherchent à dérober ces informations.

De manière générale, les cybercriminels exploitent l'intérêt des internautes à obtenir des fichiers vidéo (films, séries), des logiciels piratés (« crackés ») ou encore des programmes permettant d'améliorer les performances dans les jeux vidéo, etc.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

En partenariat avec
POLICE NATIONALE
le ministère de l'Éducation nationale et de la Jeunesse
et le ministère de la Justice

LES BONNES PRATIQUES
POUR SE PROTÉGER DES *STEALERS*

1.  Ne **pas télécharger**, ni utiliser de logiciels, d'applications et de vidéos piratés ou **d'origine douteuse** qui peuvent souvent contenir un virus.

2.  Ne **jamais désactiver votre antivirus** à la demande d'un logiciel.

3.  Face à un **message suspect** (inattendu, alarmiste, aguicheur...), **ne pas ouvrir les pièces jointes** ou cliquer sur les liens.

4.  **Mettre régulièrement à jour** vos appareils, logiciels et applications.

5.  **Utiliser des mots de passe forts** qui ne disent rien sur vous et différents pour chaque accès afin d'éviter des piratages en cascade.

6.  Deux sécurités valent mieux qu'une : **activer la double authentification** lorsque cela vous est proposé.

7.  **Ne pas stocker vos mots de passe de manière non sécurisée** : post-it, fichiers textes, messages brouillons, notes sur votre smartphone...

8.  Utiliser un **gestionnaire de mots de passe** ou un trousseau d'accès sécurisés, stockés de préférence en local, pour conserver vos mots de passe en sécurité. Vous n'aurez ainsi à retenir qu'un mot de passe pour accéder à l'ensemble de vos comptes.

9.  Ne **jamais sauvegarder vos mots de passe dans le navigateur** d'un ordinateur partagé.

10.  **Se déconnecter systématiquement de votre compte** après utilisation, pour éviter que quelqu'un puisse y accéder après vous.

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

Version 1.0