PIRATAGE D'UN SYSTÈME INFORMATIQUE

CENTRE CYBER DU PACIFIQUE

EN BREF

QU'EST-CE QUE C'EST ?

Le piratage d'un système informatique est un accès non autorisé à un appareil ou à un réseau (ordinateur, smartphone, tablette, etc.) par un tiers. Il peut résulter d'une faille de sécurité, d'un logiciel malveillant, du vol d'identifiants ou de l'usage d'un mot de passe faible ou par défaut. Une fois à l'intérieur, le cybercriminel peut prendre le contrôle de l'appareil, accéder à des informations personnelles ou confidentielles et tenter de se propager à d'autres équipements. Les données dérobées peuvent ensuite être utilisées pour l'usurpation d'identité, l'espionnage, la fraude bancaire ou d'autres usages frauduleux.

BUT RECHERCHÉ : Prendre le contrôle de l'appareil et dérober des informations personnelles ou confidentielles pour en faire un usage frauduleux.

Voici 12 bonnes pratiques à adopter si vous êtes victime

1. DÉCONNECTEZ L'APPAREIL D'INTERNET OU DU RÉSEAU
2. IDENTIFIEZ LA SOURCE DE L'INTRUSION
3. IDENTIFIEZ TOUTE ACTIVITÉ INHABITUELLE
4. ÉVALUEZ L'ÉTENDUE DE L'INTRUSION À D'AUTRES APPAREILS
5. RÉCUPÉREZ LES PREUVES
6. DÉPOSEZ PLAINTE
7. RÉALISEZ UNE ANALYSE ANTIVIRALE COMPLÈTE (SCAN)
8. SAUVEGARDEZ VOS DONNÉES PERSONNELLES
9. RÉINSTALLEZ LE SYSTÈME À PARTIR D'UNE SAUVEGARDE ANTÉRIEURE
10. CHANGEZ LES MOTS DE PASSE D'ACCÈS AUX APPAREILS TOUCHÉS
11. METTEZ À JOUR LES LOGICIELS ET APPAREILS APRÈS RÉINSTALLATION
12. FAITES-VOUS ASSISTER AU BESOIN PAR DES PROFESSIONNELS SPÉCIALISÉS

▶ Voir détail page "12 BONNES PRATIQUES À ADOPTER"

PIRATAGE D'UN SYSTÈME INFORMATIQUE

CENTRE CYBER DU PACIFIQUE

12 BONNES PRATIQUES À ADOPTER

1. DÉCONNECTEZ L'APPAREIL D'INTERNET OU DU RÉSEAU INFORMATIQUE

Déconnectez l'appareil d'Internet ou du réseau informatique.

2. IDENTIFIEZ LA SOURCE DE L'INTRUSION

Identifiez la source de l'intrusion (faille de sécurité, message malveillant…) pour la corriger afin qu'elle ne puisse pas se reproduire.

3. IDENTIFIEZ TOUTE ACTIVITÉ INHABITUELLE

Identifiez toute activité inhabituelle : nouveaux comptes utilisateurs ou administrateurs, programmes ou processus inconnus…

4. ÉVALUEZ L'ÉTENDUE DE L'INTRUSION À D'AUTRES APPAREILS

Évaluez l'étendue de l'intrusion à d'autres appareils.

5. RÉCUPÉREZ LES PREUVES

Récupérez les preuves. Mettez de côté les machines touchées à disposition des enquêteurs.

6. DÉPOSEZ PLAINTE

Déposez plainte au commissariat de police ou à la brigade de gendarmerie dont vous dépendez avec toutes les preuves en votre possession.

7. RÉALISEZ UNE ANALYSE ANTIVIRALE COMPLÈTE (SCAN)

Réalisez une analyse antivirale complète (scan) des appareils touchés afin de vérifier qu'ils ne sont pas affectés par un virus.

8. SAUVEGARDEZ VOS DONNÉES PERSONNELLES

Sauvegardez vos données personnelles (photos, vidéos, documents personnels, etc.) sur un autre support (disque dur, clef USB…).

9. RÉINSTALLEZ LE SYSTÈME À PARTIR D'UNE SAUVEGARDE ANTÉRIEURE À L'ATTAQUE

Réinstallez le système à partir d'une sauvegarde antérieure à l'attaque.

10. CHANGEZ LES MOTS DE PASSE D'ACCÈS AUX APPAREILS TOUCHÉS

Changez les mots de passe d'accès aux appareils touchés.

11. METTEZ À JOUR LES LOGICIELS ET APPAREILS APRÈS RÉINSTALLATION

Après la réinstallation de votre système mettez à jour les logiciels et appareils.

12. FAITES-VOUS ASSISTER AU BESOIN PAR DES PROFESSIONNELS SPÉCIALISÉS

Faites-vous assister au besoin par des professionnels spécialisés que vous pourrez trouver sur centrecyberpacifique.nc.

PIRATAGE D'UN SYSTÈME INFORMATIQUE

CENTRE CYBER DU PACIFIQUE

COMMENT S'EN PROTÉGER ?

Mettez à jour régulièrement votre appareil, votre système d'exploitation et ses logiciels :
pour corriger les failles de sécurité et limiter les risques d'intrusion.

Utilisez un antivirus et mettez-le à jour régulièrement :
pour détecter et neutraliser les menaces.

N'installez pas de logiciels, programmes, applications « piratées » ou dont l'origine ou la réputation sont douteuses :
pour éviter d'introduire des malwares dans votre système.

N'ouvrez pas les messages suspects, leurs pièces jointes et ne cliquez pas sur les liens :
provenant d'expéditeurs inconnus ou dont le contenu est inhabituel.

Évitez les sites non sûrs ou illicites :
tels que ceux hébergeant des contrefaçons ou certains sites pornographiques qui peuvent infecter votre machine en cours de navigation.

N'utilisez pas un compte avec des droits « administrateur » :
pour consulter vos messages ou naviguer sur Internet.

Faites des sauvegardes régulières et déconnectées de vos données et de votre système :
pour pouvoir le réinstaller au besoin.

Utilisez des mots de passe suffisamment complexes :
et changez-les au moindre doute.

Éteignez votre machine lorsque vous ne vous en servez pas :
pour limiter les risques d'accès non autorisé.

EN FONCTION DU CAS D'ESPÈCE, LES INFRACTIONS SUIVANTES PEUVENT ÊTRE RETENUES :

• L'infraction d'atteinte à un système de traitement automatisé de données (STAD) peut être retenue. Les articles 323-1 à 323-7 du code pénal disposent notamment que : « le fait d'accéder ou de se maintenir frauduleusement » dans un STAD, « la suppression ou la modification de données contenues dans le système », « le fait [...] d'extraire, de détenir, de reproduire, de transmettre [...] les données qu'il contient » ou l'« altération du fonctionnement de ce système » sont passibles de trois à cinq ans d'emprisonnement et de 100 000 à 150 000 euros d'amende.