QUELQUES CONSEILS POUR ÊTRE EN SÉCURITÉ SUR INTERNET

Une solution de sécurité de confiance
- Préférez des suites de sécurité complètes à de simples antivirus (surtout s'ils sont gratuits) qui offrent plus de fonctions pour votre sécurité.

Sauvegardez régulièrement vos données
- Réalisez des sauvegardes sur un cloud sécurisé ou sur un disque dur externe et débranchez-le quand la sauvegarde est effectuée.

Mettez à jour vos appareils
- Activez les options de mises à jour automatiques dans les paramètres de Windows, macOS, Android et iOS.

Installez vos applications uniquement depuis les sites ou magasins officiels
- Sur mobile, utilisez l'App Store ou le Google Play. Pour Windows, allez sur les sites Internet des éditeurs.

Utilisez un mot de passe différent pour chaque service
- Un gestionnaire de mots de passe gère automatiquement des identifiants différents et sécurisés.

Activez la double authentification lorsque c'est possible
- La double authentification peut se faire par SMS ou bien par application mobile.

Évitez les réseaux Wi-Fi publics ou inconnus
- Utilisez un VPN pour chiffrer votre trafic et protéger vos données.

Méfiez vous des clés et disques USB
- Certains antivirus analysent le contenu des disques USB pour plus de sécurité.

POURQUOI SE PROTÉGER CONTRE LES MENACES EN LIGNE ?

18750 nouveaux virus
et menaces apparaissent sur Internet chaque heure

650€ de rançon
à payer en moyenne pour récupérer des données prises en otage par des pirates

2,1 millions de nouveaux sites
d'hammeçonage détectés par mois

Vous cherchez une solution antivirus ?

Bitdefender

Le meilleur niveau de protection du marché

AV comparatives 2023 (1) · clubic Meilleur Antivirus 2024 (2) · AV-TEST TOP PRODUCT (3) · PC EDITORS' CHOICE (4)

(1) Bitdefender Internet Security, Janvier2024 https://www.av-comparatives.org/tests/summary-report-2023/
(2) Bitdefender Total Security, Février 2024 https://www.clubic.com/article-77079-1-guide-comparatif-meilleur-antivirus.html
(3) https://www.av-test.org/en/antivirus/home-users/
(4) https://www.pcmag.com/reviews/bitdefender-total-security

Bitdefender / FERRARI TEAM PARTNER

Bitdefender

LES RISQUES SUR INTERNET

EXPLICATIONS & CONSEILS

COMMENT VOUS PROTÉGER ?

Trusted. Always.

LES FAUX SUPPORTS TECHNIQUES

Le but de l'arnaque au faux support technique consiste à vous faire peur. Le cybercriminel vous contacte par SMS, téléphone, chat, e-mail, ou par le biais d'un message pop-up sur votre ordinateur. On vous informe d'un problème technique grave et un risque de perte de données afin de vous convaincre d'appeler un numéro de téléphone pour obtenir de l'aide*. Après avoir pris le contrôle de la machine pour faire semblant de résoudre le problème et installer des logiciels ou souscrire à des abonnements, le cybercriminel va aussi chercher à vous soutirer de l'agent en vous demandant vos coordonnées bancaires.

ARNAQUES AU SUPPORT

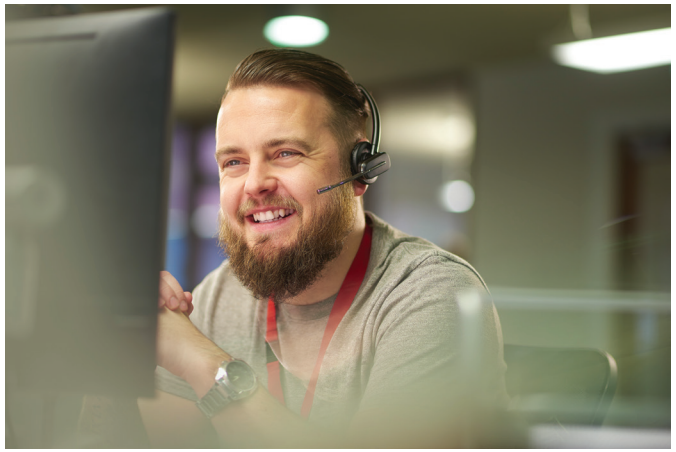
Votre ordinateur est bloqué et on vous demande de rappeler un support technique ? Vous êtes victime d'une arnaque au faux support !

BUT

Inciter la victime à payer un pseudo-dépannage informatique et/ou la faire souscrire à des abonnements payants.

TECHNIQUE

Faire croire à un problème technique grave impliquant un risque de perte de données ou d'usage de l'équipement (par écran bloqué, téléphone, SMS, courriel etc.).



CONSEILS

- Ne répondez pas au message et appels de gens que vous ne connaissez pas
- Conservez toutes les preuves
- Redémarrez votre appareil
- Faites une analyse antivirus
- Changez tous vos mots de passe
- Faites opposition auprès de votre banque si vous avez payé
- Déposez plainte

LES RANÇONGICIELS

Un rançongiciel (aussi appelé ransomware en anglais) est un logiciel malveillant qui bloque l'accès à votre appareil ou à des fichiers en les chiffrant. Le cybercriminel réclame le paiement d'une rançon pour en obtenir de nouveau l'accès. Votre appareil peut être infectée par des rançongiciels après l'ouverture d'une pièce jointe, ou après avoir cliqué sur un lien malveillant reçu dans des e-mail, ou parfois simplement en naviguant sur des sites Web compromis, ou encore suite à une intrusion sur votre système.

RANCONGICIELS

Vous ne pouvez plus accéder à vos fichiers et on vous demande une rançon ?
Vous êtes victime d'une attaque par rançongiciel !

BUT

Réclamer le paiement d'une rançon pour rendre l'accès aux fichiers verrouillés.

TECHNIQUE

Blocage de l'accès à des données par envoi d'un message contenant des liens ou pièces jointes malveillantes ou par intrusion sur le système.

CONSEILS

- Débranchez la machine d'Internet et du réseau local
- Ne payez pas la rançon
- Déposez plainte
- Faites-vous assister par des professionnels ou des connaissances expertes
- Restaurez les données à partir de vos sauvegardes

L'HAMEÇONNAGE

L'hameçonnage (aussi appelé phishing en anglais) est une fraude destinée à se faire passer pour un tiers de confiance afin de vous tromper et de vous inciter à communiquer vos données personnelles, telles que vos identifiants, vos mots de passe et/ou vos coordonnées bancaires. Il peut s'agir d'un faux message, SMS ou appel téléphonique de banque, de réseau social, d'opérateur de téléphonie, de fournisseur d'énergie, de site de commerce en ligne, d'administrations, etc.

TENTATIVES D'HAMEÇONNAGE

Vous recevez un message ou un appel inattendu, voire alarmant, d'une organisation connue et d'apparence officielle qui vous demande des informations personnelles ou bancaires ? Vous êtes peut-être victime d'une attaque par hameçonnage !

BUT

Voler des informations personnelles ou professionnelles (identité, adresses, comptes, mots de passe, données bancaires...) pour en faire un usage frauduleux.

TECHNIQUE

Leurre envoyé via un faux message, SMS, parfois par courrier postal ou appel téléphonique d'administrations, de banques, d'opérateurs, de réseaux sociaux, de sites d'e-commerce...

CONSEILS

- Ne communiquez jamais d'information sensible suite à un message ou un appel téléphonique
- Au moindre doute, contactez directement l'organisme concerné pour confirmer
- Faites opposition immédiatement (en cas d'arnaque bancaire)
- Changez vos mots de passe divulgués
- Déposez plainte
- Signalez-le sur les sites spécialisés (voir liens utiles)