Digital Security
Progress. Protected.

ÉDITION
2023

SOLUTIONS DE SÉCURITÉ MULTIPLATEFORMES

Particuliers & TPE

ADOPTEZ LES BONS REFLEXES

Utilisez des mots de passe uniques, forts et complexes

- Changez les mots de passe par défaut des services auxquels vous accédez
- Utilisez au minimum 12 caractères dont des minuscules, des majuscules, des chiffres et des symboles

Sécurisez l'accès à vos appareils mobiles et objets connectés

- Changez les identifiants par défaut de vos objets connectés
- Ne partagez l'accès à votre Wi-Fi qu'avec vos proches

Ne diffusez pas vos informations personnelles sur Internet

- Gérez vos paramètres de confidentialité pour ne pas divulguer vos informations privées (informations bancaires, adresses, photos...)
- Pensez à vous déconnecter de votre compte sur les ordinateurs publics

Méfiez-vous des emails suspects / frauduleux

- Détectez les faux courriels et classez-les dans vos courriers indésirables
- En cas de réception d'un message contenant un lien, positionnez le curseur de la souris (sans cliquer) sur ce lien pour afficher l'adresse vers laquelle il pointe réellement

Appliquez les mises à jour de vos appareils et logiciels

- En général, les mises à jour de versions apportent de nouvelles fonctionnalités tout en corrigeant des failles de securité
- Téléchargez vos mises à jour uniquement depuis les sites officiels

Effectuez des sauvegardes régulières de vos données

- Pensez à tester vos sauvegardes
- En cas de perte, de vol, de panne, de piratage ou de destruction de vos appareils numériques, vous perdrez les données enregistrées sur ces supports

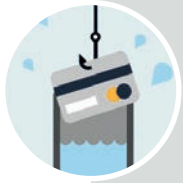
POUR MIEUX SE PROTÉGER CONTRE LES MENACES

USURPATION D'IDENTITÉ

Les cybercriminels recherchent des informations confidentielles (mots de passe, numéros de cartes de crédit, numéros de sécurité sociale...), qu'ils peuvent utiliser à des fins illégales (prêts, achats en ligne, revente de données...). Un crime grave et lourd de conséquences pour les victimes.

RANSOMWARE

Le rançongiciel est un logiciel malveillant qui peut verrouiller l'accès à un appareil ou en chiffrer le contenu, dans le but de vous extorquer de l'argent. Les cybercriminels promettent, sans garantie bien sûr, de restaurer l'accès à votre machine et aux données affectées une fois la rançon payée.



PHISHING

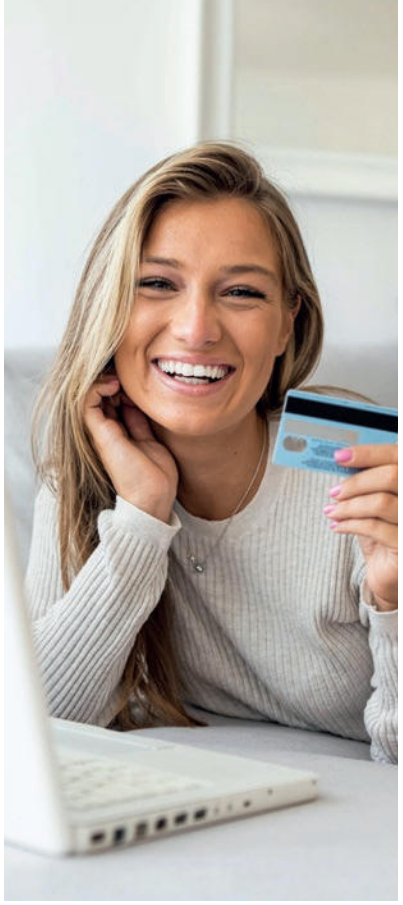
L'hameçonnage est une technique consistant à se faire passer pour une personne ou une entité en qui vous avez toute confiance, afin de vous soutirer des informations sensibles ou personnelles. Cela prend le plus souvent la forme d'un e-mail de votre banque ou d'un autre service en ligne à l'apparence parfaitement authentique.

SPAM

Très répandu depuis des décennies (le premier spam connu date de 1978), le spam est un e-mail ou tout type de message numérique que vous n'avez pas sollicité. Souvent irritant et ennuyeux, parfois dangereux, il faut savoir s'en prémunir.

INTRUSION

L'intrusion consiste à pénétrer votre réseau sans autorisation afin d'en prendre le contrôle et d'exploiter les fichiers et les informations stockées sur vos appareils. Protégez-vous avec un pare-feu efficace et des protections additionnelles tel qu'une protection contre les attaques Brute Force



ADVANCED SECURITY

ESET INTERNET SECURITY

Rapide, léger et complet

La sécurité de votre famille est notre priorité. Idéale pour protéger votre foyer, cette suite de sécurité combine notre antivirus NOD32 à de nombreuses fonctionnalités additionnelles pour protéger l'ensemble de votre univers numérique.

Elle est complète, fiable et veille sur vos données personnelles et bancaires. Elle protège vos appareils intelligents et votre maison connectée tandis que le module de contrôle parental vous permet de sécuriser la navigation de vos enfants sur Internet. Sécurisez votre vie privée et votre foyer en quelques clics !

LES NOUVEAUTÉS

La technologie Intel® Threat Detection Technology (Intel® TDT) permet de surveiller les cyberattaques et d'améliorer les performances de sécurité au niveau matériel. La solution ESET marche de pair avec la technologie Intel® TDT pour découvrir des attaques avancées qui échappent à la plupart des autres méthodes de détection.

La protection des attaques de type Brute Force vous protège des tentatives d'intrusion qui consiste à utiliser un grand nombre de suite de caractère et de chiffre pour déceler votre mot de passe.

LE LÉGENDAIRE MOTEUR NOD32

Depuis 1987, le moteur NOD32 ne cesse d'innover pour vous offrir le ciment essentiel à votre sécurité informatique. Il alimente l'ensemble de nos suites de sécurité en associant protection maximale, ergonomie et faible impact système. Nos technologies avancées utilisent l'intelligence artificielle pour empêcher l'infiltration de virus, de logiciels espions, de chevaux de Troie, d'adwares, de rootkits et de bien d'autres menaces, sans pour autant ralentir votre ordinateur.

Protection des données bancaires

Bénéficiez de nos différents outils de sécurité des données bancaires dont un navigateur sécurisé pour effectuer vos paiements en ligne et la protection automatique de vos opérations bancaires sur Internet. Les communications entre le clavier et le navigateur seront chiffrées pour des transactions plus sûres.

Surveillance des objets connectés

Gardez l'oeil sur tous vos appareils intelligents et connectés grâce à notre fonctionnalité "Network Inspector". Testez votre routeur, détectez des vulnérabilités telles que des mots de passe faibles et suggérez des options pour résoudre des éventuels problèmes afin d'améliorer la sécurité globale de votre foyer. Cela vous permets de détecter si un utilisateur inconnu est connecté à votre réseau.

Contrôle parental

Protégez vos enfants des contenus inadaptés en ligne et administrez une liste noire personnalisée. Vous avez la possibilité de définir des contrôles pour la durée d'utilisation des applications ou des jeux. pour chaque enfant, ou bloquez complètement les applications inappropriées. En cas d'urgence, Vous pouvez retrouver votre enfant grâce à la localisation de son appareil connecté à Internet.

Intel Threat Detection Technology NOUVEAUTÉ

Anti-hameçonnage

Protection Multicouche

Protection des attaques de type Brute Force NOUVEAUTÉ

Faible impact système