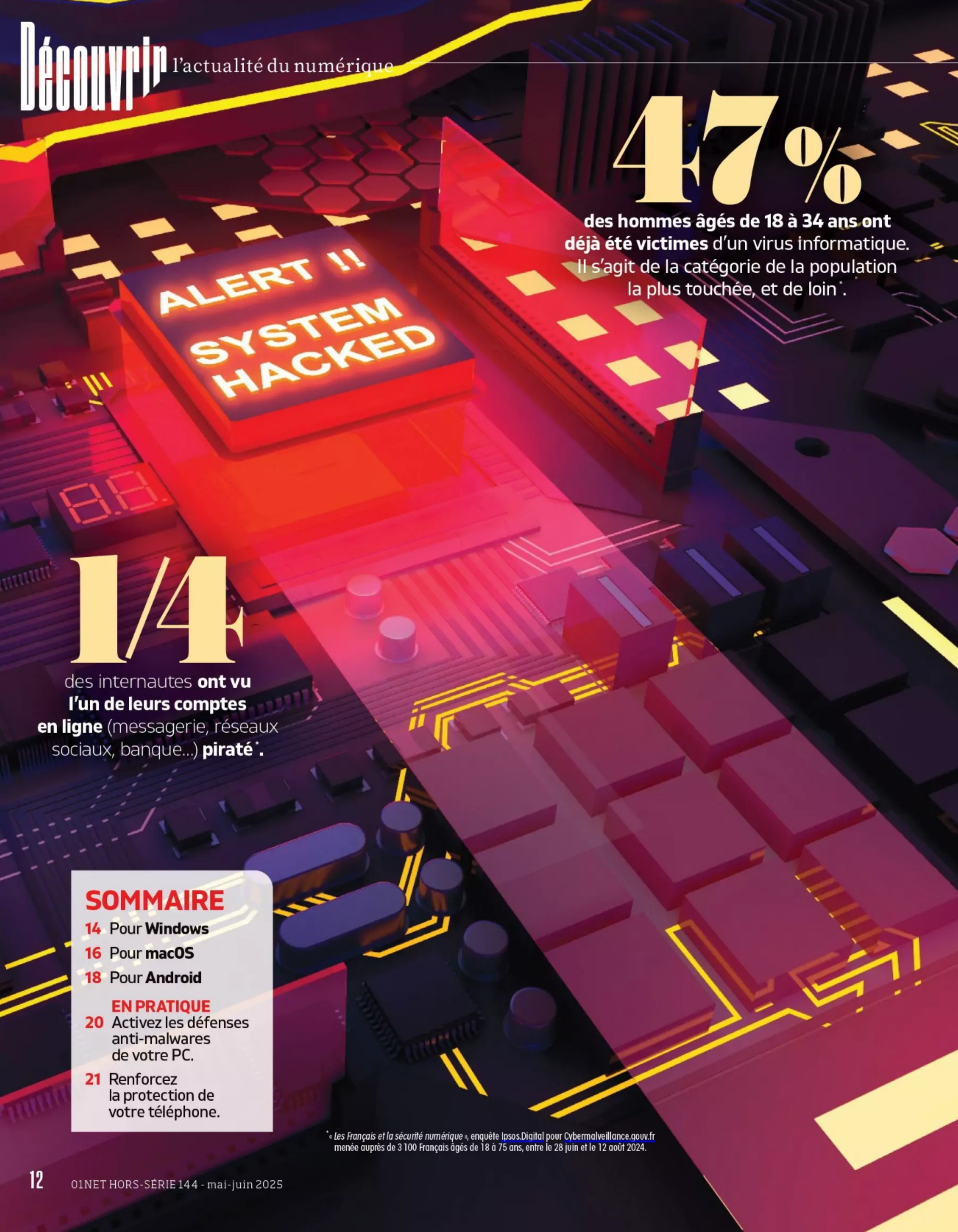


47 %

des hommes âgés de 18 à 34 ans ont déjà été victimes d'un virus informatique. Il s'agit de la catégorie de la population la plus touchée, et de loin*.

1/4

des internautes **ont vu l'un de leurs comptes en ligne** (messagerie, réseaux sociaux, banque…) **piraté*.**

SOMMAIRE

14 Pour **Windows**
16 Pour **macOS**
18 Pour **Android**

EN PRATIQUE
20 Activez les défenses anti-malwares de votre PC.
21 Renforcez la protection de votre téléphone.

* « *Les Français et la sécurité numérique* », enquête Ipsos.Digital pour Cybermalveillance.gouv.fr menée auprès de 3 100 Français âgés de 18 à 75 ans, entre le 28 juin et le 12 août 2024.

OSELOTE/ISTOCKPHOTO

PC, MAC, SMARTPHONES

LES MEILLEURES SUITES ANTIVIRUS 2025

La cybersécurité n'est plus une option. Car la menace vise désormais tous nos appareils, du smartphone à l'ordinateur en passant par les objets connectés.

Imaginez-vous un instant perdre l'accès à votre compte bancaire, être dépossédé de vos économies à cause d'un faux lien ou encore voir vos échanges privés exposés publiquement. Ces scénarios, autrefois rares, sont devenus monnaie courante. En 2023, les forces de sécurité intérieure ont enregistré 278 770 infractions liées au numérique*, soit une hausse de 40 % en cinq ans. 59 % d'entre elles relevaient d'atteintes aux biens, telles que des escroqueries et arnaques en ligne, et 34,5 % d'atteintes aux personnes, de la diffusion de contenus pédopornographiques au cyberharcèlement.

Depuis l'apparition des premiers virus informatiques, dans les années 1980, les cyberattaques ont bien changé. Aujourd'hui, elles prennent des formes multiples et sophistiquées, comme les rançongiciels (qui bloquent l'accès à des données jusqu'au paiement d'une rançon) ou le *smishing* (contraction des mots SMS et *phishing*), qui désigne le vol de données sensibles (numéros de cartes bancaires, identifiants, etc.) par l'envoi de messages sur le téléphone de la victime, l'expéditeur se faisant souvent passer pour une entité légitime. Face à cette évolution, une seule conclusion s'impose : en plus d'une sensibilisation accrue à ces menaces, il est indispensable de se protéger efficacement. C'est-à-dire de se prémunir contre les virus, c'est la base, mais aussi idéalement de se camoufler derrière le paravent d'un réseau privé virtuel (VPN), tout en préservant les enfants à l'aide d'un contrôle parental. De même faut-il réduire les risques liés au « facteur humain » en confiant la gestion de ses mots de passe à un outil ad hoc.

Des solutions clés en main

Il y a alors deux façons de procéder. La première consiste à sélectionner séparément un outil pour faire face à chaque menace, soit : un pare-feu, un antivirus, un filtre anti-*malwares* (logiciels malveillants), une protection des paiements en ligne, un VPN, un système antispam pour protéger sa messagerie, une solution de contrôle parental et une autre pour gérer les mots de passe. La seconde option revient à s'en remettre à une suite de sécurité qui comprend tout ou partie de ces briques de protection. Ce sont ces solutions que nous avons choisi ici de comparer en nous appuyant sur les tests rigoureux du laboratoire indépendant AV-Test, et en prenant en compte la présence d'une solution VPN, de protection parentale ou de gestion des mots de passe. Mais entendons-nous bien, le problème n'est pas tellement de tomber sur un mauvais antivirus. Tous font, globalement, parfaitement l'affaire. Non, la difficulté est aujourd'hui de se protéger sur tous les fronts. ■■■

11 SUITES DE SÉCURITÉ POUR WINDOWS

Aujourd'hui, une suite de sécurité ne peut plus se contenter d'un pare-feu et d'un antivirus. Un contrôle parental, un gestionnaire de

LOGICIEL / CARACTÉRISTIQUES		KASPERSKY PLUS	ESET HOME SECURITY ULTIMATE	MCAFEE TOTAL PROTECTION	F-SECURE TOTAL	BITDEFENDER TOTAL SECURITY
Site internet		bit.ly/4j08h7x	bit.ly/3WA13tP	bit.ly/4ØvAkj2	bit.ly/3PRf7LJ	bit.ly/4hmsQps
Protection contre les logiciels malveillants*		6/6	6/6	6/6	6/6	6/6
Impact sur les performances du PC*		6/6	6/6	6/6	5,5/6	5,5/6
Capacité à ne pas alerter inutilement*		6/6	6/6	5,5/6	6/6	6/6
VPN		OUI	OUI	OUI	OUI	OUI (200 Mo/jour)**
Contrôle parental		OUI	OUI	OUI VERSION FAMILIALE	OUI	OUI VERSION FAMILY
Gestionnaire de mots de passe		OUI	OUI	OUI	OUI	OUI
Prix annuel pour 1 appareil	PREMIÈRE ANNÉE	30 €	—	—	70 €	—
	DEUXIÈME ANNÉE	55 €				
Prix annuel pour 5 appareils	PREMIÈRE ANNÉE	40 €	120 €	40 €	100 €	50 €
	DEUXIÈME ANNÉE	80 €		110 €		95 €
VERDICT		9,5/10	9/10	9/10	9/10	9/10
NOTRE AVIS		Banni pour les fonctionnaires aux Pays-Bas ou aux États-Unis, l'antivirus russe n'en reste pas moins LA référence pour les particuliers.	Eset vient concurrencer les grands noms du secteur avec une suite complète et efficace. Mais pas la moins chère.	Pour AV-Test, cet antivirus excelle auprès des particuliers avec son faible impact sur les performances de Windows.	Un léger impact sur les performances empêche F-Secure de se hisser parmi les tout meilleurs.	Solution la plus saluée par AV-Test pour les entreprises, Bitdefender pêche seulement par son léger impact sur les performances des PC des particuliers.

▪▪▪ Un premier constat s'impose à nous : aucun des antivirus passés au crible d'AV-Test, sous Windows 10 et 11, macOS ou Android, n'a failli. Tous parviennent, à quelques exceptions près, à bloquer les attaques simulées par le laboratoire indépendant. Pourtant, dans le détail, tous ne se valent pas. Il existe des différences d'approche. Bitdefender et Kaspersky excellent, par exemple, dans l'exercice qui consiste à bloquer les vulnérabilités dites « *zero day* ». Le terme fait référence à une faille n'ayant pas encore été découverte par le développeur d'un programme, mais potentiellement exploitée par des personnes malveillantes. L'expression reflète l'urgence de la situation, car le développeur n'a eu aucun jour (zéro) pour déployer un correctif. Un autre point différenciant concerne l'utilisation de l'intelligence artificielle pour détecter de nouvelles menaces.

L'IA peut s'alerter d'anomalies et couper court à des attaques non encore répertoriées.

L'intelligence artificielle contre les malwares

Habituellement, lorsqu'un *malware* est découvert, les éditeurs d'antivirus analysent son code et en tirent une signature, qu'ils ajoutent à une base de données. Quand la suite de sécurité scanne les fichiers ou les processus en cours d'exécution, toute correspondance indique qu'une menace est présente. Si ce système jouit d'une grande précision et s'avère très fiable, il ne saurait, en revanche, reconnaître un programme malveillant qui n'est pas catalogué. C'est là que l'IA entre en jeu. En

mots de passe et un VPN sont des briques de sécurité indispensables.

AVAST ONE BASIC	NORTON 360	G DATA TOTAL SECURITY	AVIRA INTERNET SECURITY	MICROSOFT DEFENDER ANTIVIRUS	AVG INTERNET SECURITY
bit.ly/4aHZKig	bit.ly/4hw1zkz	bit.ly/4hBJ3Hv	bit.ly/42NaqKD	bit.ly/4h09lFD	bit.ly/4jtvo75
6/6	6/6	6/6	6/6	6/6	6/6
6/6	5,5/6	6/6	6/6	6/6	6/6
6/6	6/6	6/6	6/6	6/6	6/6
OUI (5 Go/semaine)**	OUI	OUI (+30 €)	NON	NON	NON
NON	OUI VERSION DELUXE	OUI	NON	OUI	NON
OUI	OUI	OUI	OUI	NON	NON
Gratuit	**30 €** VERSION STANDARD **75 €** VERSION STANDARD	**50 €**	**27 €** **55 €**	**Inclus avec Windows 11**	**35 €** **73 €**
57 € VERSION SILVER **115 €** VERSION SILVER	**35 €** VERSION DELUXE **105 €** VERSION DELUXE	**82 €**	**75 €**	**99 €** MICROSOFT 365 PERSONNEL	**60 €** 10 APPAREILS **94 €** 10 APPAREILS
8,5/10	**8,5/10**	**8,5/10**	**8/10**	**8/10**	**7/10**
Malgré l'absence de contrôle parental et le VPN limité, la version gratuite assure bien plus que l'essentiel. La version payante est chère.	Malgré son impact sur les performances du PC, Norton 360 demeure, avec son excellent VPN, une référence. Très complet.	Dommage que le VPN ne soit pas inclu dans le prix de base. Il coûte 30 € par an si acheté en même temps que la suite, ou le double !	Efficace, mais l'absence de contrôle parental et de VPN nous pousse à conseiller d'autres produits plus complets.	Si l'antivirus de Windows disposait d'un gestionnaire de mots de passe, il pourrait se suffire à lui-même. À compléter avec le VPN de Edge.	Dépourvu de gestionnaire de mots de passe, de contrôle parental et de VPN, ce dernier étant vendu à part 60 € par an. Dommage…

* Scores AV-Test publiés au mois d'octobre 2024 pour Windows 11. ** Illimité dès la version premium.

LE POINT MÉTHODO

Pour tout ce qui concerne la protection sous Windows 11, nous nous sommes appuyés sur le laboratoire AV-Test. Ses scores (dont certaines valeurs non incluses dans ce tableau) comptent pour 70 % de notre note verdict. Afin de compléter notre moyenne pondérée, nous avons compté pour 15 % la présence d'un VPN, pour 10 % celle d'un gestionnaire de mots de passe et pour 5 % le contrôle parental. Le prix de la solution joue aussi sur le classement.

surveillant en temps réel les actions des fichiers ou des programmes, comme certaines modifications non autorisées ou l'accès à des données sensibles, elle peut s'alerter de manière proactive d'anomalies et couper court à des attaques non encore répertoriées. Pour distinguer les programmes malveillants des programmes légitimes, et bloquer autant que faire se peut les premiers, l'IA s'entraîne sur de gigantesques ensembles de données qu'elle traite au moyen du « *machine learning* », autrement dit des algorithmes d'apprentissage automatique. La suite Norton 360, entre autres, met à profit ces techniques avancées.

La bourse ou les données ?

Un autre sujet d'inquiétude est celui des rançongiciels, dont de nombreux hôpitaux ont fait les (très gros) frais ces dernières années. Les particuliers ne sont pas épargnés, loin de là. L'inoculation suit toujours les mêmes scénarios : ouverture d'une pièce jointe malveillante dans un mail, clic sur un mauvais lien… Le but est d'installer un *malware* qui, en arrière-plan, va chiffrer tout ou partie des données, rendant leur ouverture future impossible à qui ne détient pas la fameuse clé. Le détenteur de cette dernière étant, bien entendu, le pirate informatique. Pire, certains rançongiciels savent se propager à d'autres appareils connectés au même réseau. À la perte de ses photos de famille et de ses documents personnels s'ajoute un stress important. Et il n'est nullement garanti qu'en payant la rançon exigée – quelques centaines, voire milliers d'euros –, l'accès à ces précieuses données soit restitué. Heureusement, là encore, la technologie vient limiter les dégâts de ce qui reste, au départ, ■■■

9 SUITES DE SÉCURITÉ POUR MACOS

À l'heure des rançongiciels et des *malwares*, les appareils d'Apple ne peuvent plus se contenter d'un pare-feu et d'un antivirus.

LOGICIEL / CARACTÉRISTIQUES		NORTON 360	KASPERSKY PREMIUM	BITDEFENDER TOTAL SECURITY	AVAST ONE BASIC
Site internet		bit.ly/4hw1zkz	bit.ly/3PQMjmy	bit.ly/4hmsQps	bit.ly/4autj6J
Protection contre les logiciels malveillants*		6/6	6/6	6/6	6/6
Impact sur les performances du Mac*		6/6	6/6	6/6	6/6
Capacité à ne pas alerter inutilement*		6/6	6/6	6/6	6/6
VPN		OUI	OUI	OUI (200 Mo/jour)**	OUI (5 Go/semaine)**
Contrôle parental		OUI VERSION DELUXE	OUI	OUI VERSION FAMILY	NON
Gestionnaire de mots de passe		OUI	OUI	OUI	OUI
Prix annuel pour 1 appareil	PREMIÈRE ANNÉE	30 € VERSION STANDARD	40 €	—	Gratuit
	DEUXIÈME ANNÉE	75 € VERSION STANDARD	80 €		
Prix annuel pour 5 appareils	PREMIÈRE ANNÉE	35 € VERSION DELUXE	55 €	50 €	57 € VERSION SILVER
	DEUXIÈME ANNÉE	105 € VERSION DELUXE	100 €	95 €	115 € VERSION SILVER
NOTE GLOBALE		10/10	9,5/10	9/10	8,5/10
NOTRE AVIS		Norton 360 l'emporte grâce à un léger avantage tarifaire sur la suite de Kaspersky.	L'antivirus russe, bien que déconseillé par certains États européens, reste l'un des meilleurs auprès des particuliers.	Très bonne et très complète. Dommage que le VPN soit très limité dans la version de base.	L'absence de contrôle parental pénalise Avast. On regrette le tarif plutôt élevé des versions premiums.

■■■ une erreur humaine. Selon AV-Test, les suites de sécurité de ce comparatif s'en sortent globalement très bien, avec une mention spéciale, sous Windows, pour Bitdefender, Eset, McAfee et Microsoft Defender, qui ont stoppé tous les rançongiciels qui leur ont été soumis en décembre 2024. Plus embêtant, Avira n'a, lui, pas réussi à bloquer deux attaques sur les dix scénarios testés. Point de panique, cependant, si vous êtes équipé de cette solution. Il n'y a vraiment pas péril en la demeure et le niveau de protection globale reste très élevé. D'ailleurs, AV-Test lui octroie tout de même sa note maximale sous Windows (100 % de protection contre les attaques « *zero day* » et les logiciels malveillants les plus répandus). C'est plutôt sous macOS et Android qu'il s'avère moins efficace (avec un score de protection de « seulement » 99,5 % et 99,9 % respectivement).

Un VPN augmente la sécurité en ligne en dissimulant votre adresse IP.

Naviguez heureux, naviguez caché

Si nous avons aussi choisi d'intégrer à notre comparatif le VPN, ce n'est pas parce que nous avons des choses à cacher, mais bien parce que cet outil est devenu réellement indispensable. Le principe est de créer une connexion chiffrée entre votre appareil et un serveur distant. Outre le fait de faire croire à un service, par exemple de vidéo à la demande, que l'on se trouve aux États-Unis alors que l'on est en France, ce type de logiciel ou d'application augmente la sécurité en ligne en dissimulant son adresse IP. Mais comment s'équiper ? D'abord, certains sont accessibles gratuitement, tels Hide.me, Proton VPN, TunnelBear ou celui intégré au navigateur internet Opera. Le

F-SECURE TOTAL	TOTALAV TOTAL SECURITY	AVIRA INTERNET SECURITY	AVG INTERNET SECURITY	INTEGO MAC PREMIUM BUNDLE X9
bit.ly/3PRf7LJ	bit.ly/3WA2TKU	bit.ly/3Eb4L6F	bit.ly/3PRrnM8	bit.ly/4hbj89P
6/6	5,5/6	5,5/6	6/6	5/6
6/6	6/6	6/6	6/6	6/6
6/6	6/6	6/6	6/6	6/6
OUI	OUI	NON	NON	NON
OUI	NON	NON	NON	OUI
OUI	OUI	OUI	NON	NON
70 €	—	27 €	35 €	70 €
		55 €	73 €	85 €
100 €	49 € 8 APPAREILS	75 €	60 € 10 APPAREILS	120 €
	149 € 8 APPAREILS		94 € 10 APPAREILS	147 €
8,5/10	7,5/10	7/10	7/10	6/10
Une très bonne suite, mais qui monnaye plus cher ses services. Sans tarif préférentiel la première année.	Quelques fausses alertes de l'antivirus et l'absence de contrôle parental affectent sa note. Dommage.	De petites erreurs de détection, pas de contrôle parental et un VPN très limité (500 Mo/mois) qui s'installe séparément.	Bonne suite, mais pas de VPN, de gestionnaire de mots de passe et de contrôle parental. Regrettable.	Un chouia en dessous niveau protection, mais l'interface a été conçue pour le Mac, et ça se voit. Tarif plutôt élevé.

* Scores AV-Test publiés au mois de décembre 2024, et septembre 2024 dans le cas d'Intego. ** Illimité en version premium.

LE POINT MÉTHODO

Pour tout ce qui concerne la protection sous macOS Sonoma, nous nous sommes appuyés sur le laboratoire AV-Test. Ses scores (dont certaines valeurs non incluses dans ce tableau) comptent pour 70 % de la note verdict. Afin de compléter notre moyenne pondérée, nous avons compté pour 15 % la présence d'un VPN, pour 10 % celle d'un gestionnaire de mots de passe et enfin pour 5 % le contrôle parental. Le prix de la solution joue aussi sur le classement.

problème reste qu'ils sont limités et proposent généralement des débits médiocres. Cela permet d'avancer masqué, mais au ralenti. Pour une utilisation autre que ponctuelle, on peut s'en remettre aux spécialistes que sont CyberGhost, ExpressVPN ou NordVPN. Après une période d'essai d'un mois, ils basculent sur un abonnement souvent modique, de l'ordre de quelques euros mensuels avec un engagement sur plusieurs mois, voire plusieurs années. Efficaces et rapides, nous ne pouvons que les conseiller. Dernière option : beaucoup de suites de sécurité intègrent leur propre solution de VPN. Par rapport aux logiciels spécialisés, on note un nombre inférieur de serveurs et donc de localisations possibles, ce qui, sauf besoins spécifiques, est de peu d'importance. Avec Bitdefender, Norton ou Kaspersky, la vitesse de connexion est au rendez-vous, ce qui reste essentiel. Pour une meilleure protection, tous possèdent une fonction ▪▪▪

COMMENT PAYER BEAUCOUP MOINS CHER

Si vous observez nos tableaux, vous verrez que le tarif bondit après la première année d'abonnement. Mais il existe une astuce pour payer moins cher. Tous les éditeurs sont contraints par le Code de la consommation à informer un mois avant la date anniversaire de la tacite reconduction du contrat pour permettre une éventuelle résiliation. C'est là qu'il faut agir, se rendre dans son espace client et supprimer cette tacite reconduction. Il y a alors fort à parier que vous receviez des offres avantageuses (nous l'avons vérifié avec Bitdefender et Kaspersky) pour vous convaincre de rester. Pour payer encore moins cher, vous pouvez aussi vous en remettre aux outils délivrés avec votre système d'exploitation. Windows Defender obtient ainsi la note maximale en matière de protection contre les virus. Microsoft propose également Secure Network, un VPN intégré au navigateur Edge, et Microsoft Family Safety, un système de contrôle parental pour restreindre les paiements ou le temps d'écran. Côté Mac, XProtect (anti-*malware*) et Gatekeeper (contrôle des applications) fournissent un degré minimal de protection.

9 SUITES DE SÉCURITÉ POUR ANDROID

La gratuité a encore cours au sein des suites de sécurité pour Android. Mais les versions payantes ajoutent des fonctions supplémentaires :

LOGICIEL / CARACTÉRISTIQUES		BITDEFENDER MOBILE SECURITY	F-SECURE TOTAL SECURITY & VPN	MCAFEE SECURITY : ANTIVIRUS VPN	KASPERSKY PREMIUM	ESET MOBILE SECURITY ANTIVIRUS	NORTON 360
Site internet		bit.ly/4azernC	bit.ly/4ØMLykq	bit.ly/4ØYOZVD	bit.ly/4gvNP8B	bit.ly/4aFy6m4	bit.ly/4hw1zkz
Protection contre les logiciels malveillants*		6/6	6/6	6/6	6/6	6/6	6/6
Impact sur les performances du smartphone*		6/6	6/6	6/6	6/6	6/6	6/6
Capacité à ne pas alerter inutilement*		6/6	6/6	6/6	6/6	6/6	6/6
VPN		OUI (200 Mo/jour) **	OUI	OUI	OUI	NON	OUI
Fonction antivol		OUI	OUI	OUI	OUI	OUI	NON
Prix annuel	PREMIÈRE ANNÉE	15 €	20 €	65 €	35 €	10 €	30 €
	DEUXIÈME ANNÉE	25 €			80 €		75 €
NOTE GLOBALE		10/10	9,5/10	9,5/10	9/10	9/10	9/10
NOTRE AVIS		Pour AV-Test, il s'agit de la meilleure suite Android pour les particuliers (award 2024).	Le VPN illimité est son point fort, idéal pour le streaming.	Une protection complète, mais un tarif très élevé face aux concurrents. Le VPN est illimité.	Bien qu'exclu du Play Store, Kaspersky n'en demeure pas moins recommandable selon nous.	Interface claire, protection au top et faible impact sur l'autonomie, il ne manque	Norton reste une référence aussi du côté des mobiles (même offre sous iOS). Manque

▪▪▪ « *kill switch* », qui bloque automatiquement tout le trafic internet de votre appareil si la connexion VPN est interrompue. Bon à savoir, certains services, notamment bancaires, n'apprécient pas ce type de connexions anonymisées et vous bloqueront l'accès. Il faudra désactiver votre VPN le temps de les utiliser.

Ne pas oublier le smartphone

Un peu plus d'un Français sur deux déclare avoir installé un « logiciel antivirus » sur son smartphone, d'après un sondage réalisé par Bitdefender entre décembre 2023 et janvier 2024. Un choix judicieux puisque, selon Thalès, près de 34 millions de cyberattaques ciblant des appareils mobiles ont été recensées dans le monde en 2023, dont plus de 300000 en France. Entre les mails frauduleux, les arnaques sur les réseaux sociaux et les appels indésirables, la réalité nous rappelle constamment qu'employer notre mobile expose à des risques. L'« ingénierie sociale », autrement dit la manipulation psychologique utilisée par des individus malveillants pour inciter des personnes à divulguer des informations confidentielles, joue un rôle essentiel. L'hameçonnage (*phishing*) passe ici par les messageries, mais aussi par la voix (*vishing*) et les SMS (*smishing*). Pour les malfaiteurs, la manœuvre consiste à se faire passer pour un tiers de confiance, soit le représentant d'une institution ou d'une société, soit pour un membre de la famille. Ensuite, c'est un aller simple vers l'arnaque, avec à la clé le vol de données personnelles et celui, pur et simple, de son argent. La première chose à comprendre, même si le cas moqué sur les réseaux de cette dame qui a lâché 830000 euros à un faux Brad Pitt semble paroxystique, est que cela n'arrive pas qu'aux autres. Avec le développement de l'IA générative, les vidéos d'un faux Florent Pagny (bit.ly/4qbsEbq) en témoignent. Le chanteur a dénoncé lui-même la supercherie auprès de TF1, soulignant à quel point

Plus de 300 000 cyberattaques ciblant des mobiles ont été recensées en France en 2023.

VPN plus rapide, protection des paiements en ligne...

AVAST ANTIVIRUS & SÉCURITÉ	AVG ANTIVIRUS GRATUIT	AVIRA ANTIVIRUS SECURITY
bit.ly/4ØQjDQV	bit.ly/4gvftm9	bit.ly/4ØPdjcr
6/6	6/6	6/6
6/6	6/6	6/6
6/6	6/6	5/6
OUI VERSION PREMIUM	OUI VERSION ULTIMATE	OUI (100 Mo/jour)
NON	NON	OUI
Gratuit	**Gratuit**	**Gratuit**
9/10	**9/10**	**8/10**
L'un des antivirus les plus utilisés au monde. La version avec VPN coûte 42 € la première année, puis 94 €.	Le VPN est inclus dans la version la plus chère (80 € puis 130 €/an), ainsi que l'optimisation des performances.	Si la version gratuite est bien, l'offre Phantom Pro (4,95 €/mois) ajoute un VPN illimité. Interface limpide.

* Scores AV-Test de janvier 2025. ** Illimité en version premium (70€ puis 110 €/an).

LE POINT MÉTHODO

Pour comparer les suites de sécurité qui sont dévolues aux smartphones, nous nous sommes appuyés sur les mesures d'AV-Test. Ils ne concernent que les appareils Android, puisque les iPhone répondent à une autre logique sécuritaire. Nous avons noté la protection contre les malwares à hauteur de 70 % de la note finale et ajouté 15 % pour le VPN intégré et autant pour la fonction antivol. Le prix de la solution joue aussi sur le classement.

son apparence et sa voix étaient bien imitées. En dehors d'une méfiance salutaire, les suites de sécurité peuvent donc aider. Mais si la tromperie concerne autant les possesseurs d'iPhone que de téléphones Android, il existe une grande différence de conception logicielle.

Android et iOS pas égaux

C'est une forme d'injustice ou peut-être le prix de la liberté face à l'écosystème fermé d'Apple, argueront les défenseurs d'Android. Mais c'est un fait, les iPhone sont moins susceptibles de subir des attaques virales que les autres smartphones. Plusieurs raisons expliquent cela. Premièrement, iOS recourt à un système dit de « bac à sable », où chaque application fonctionne en silo. Cela signifie qu'elle ne peut pas interagir directement avec d'autres ou accéder au système d'exploitation sans autorisation. Deuxièmement, l'App Store est très sécurisé, ce qui pourrait malgré tout changer avec l'avènement de magasins alternatifs imposé par la Commission européenne. Enfin, et surtout, Apple centralise et coordonne des mises à jour logicielles pour une gamme limitée d'appareils, les siens, et propose un suivi à très long terme. De l'autre côté, l'architecture logicielle plus ouverte d'Android, avec un Play Store moins contrôlé et une plus grande liberté dans les permissions accordées aux applications, se trouve plus souvent mise en défaut. La différence rappelle finalement celle qui existe entre Windows et un macOS naturellement mieux immunisé.

Un antivol renforcé

L'autre risque est bien sûr de se faire subtiliser son mobile. Si voler un iPhone verrouillé peut sembler vain puisque le malfaiteur se retrouvera avec une « brique », il peut y trouver un intérêt. On pense à la revente frauduleuse, parfois à destination de l'étranger, et à la vente pour pièces détachées. Sous iOS comme sous Android, les fonctions de localisation natives sont suffisantes. Elles permettent de géolocaliser l'appareil en temps réel, de le faire sonner à plein volume, de verrouiller l'écran et d'effacer toutes les données à distance. Pour les iPhone, un mode « Perdu » affiche en outre les coordonnées du propriétaire. Les suites de sécurité proposant une fonction antivol permettent un suivi en temps réel de l'appareil sur une carte interactive, mais aussi d'être notifié en cas de changement de carte SIM et de déclencher l'appareil photo pour espérer prendre un cliché du voleur qui essaie de déverrouiller le smartphone. Des fonctions certes inintéressantes, mais qui ne garantissent en rien le retour de son mobile chéri. ●

* D'après le « Rapport annuel sur la cybercriminalité 2024 » du Commandement du ministère de l'Intérieur dans le cyberespace.

UNE BOX POUR LES OBJETS CONNECTÉS ?

Il y a quelques années, des box spécialisées dans la sécurité des appareils connectés étaient vendues par Bitdefender et F-Secure. Alors que les objets connectés pullulent dans nos foyers et se font vecteurs de nouvelles attaques, ces appareils sont en fin de vie et indisponibles à la vente. À la place, Bitdefender préfère travailler avec l'équipementier Netgear pour intégrer dans ses routeurs ses solutions de sécurité. Pour limiter les risques, sachant que nombre de ces accessoires connectés comportent des failles de sécurité, nous conseillons, si possible, de créer un réseau Wifi réservé, distinct de celui utilisé par les ordinateurs, smartphones ou tablettes de la maison. Pour surveiller le réseau domestique, beaucoup de suites de sécurité telles que Bitdefender, Kaspersky, Norton, McAfee ou Trend Micro intègrent ce type de monitoring.

DIFFICULTÉ **MODÉRÉE** TEMPS **20 MIN** DOMAINE **SÉCURITÉ**

ACTIVEZ LES DÉFENSES ANTIMALWARES DE VOTRE PC

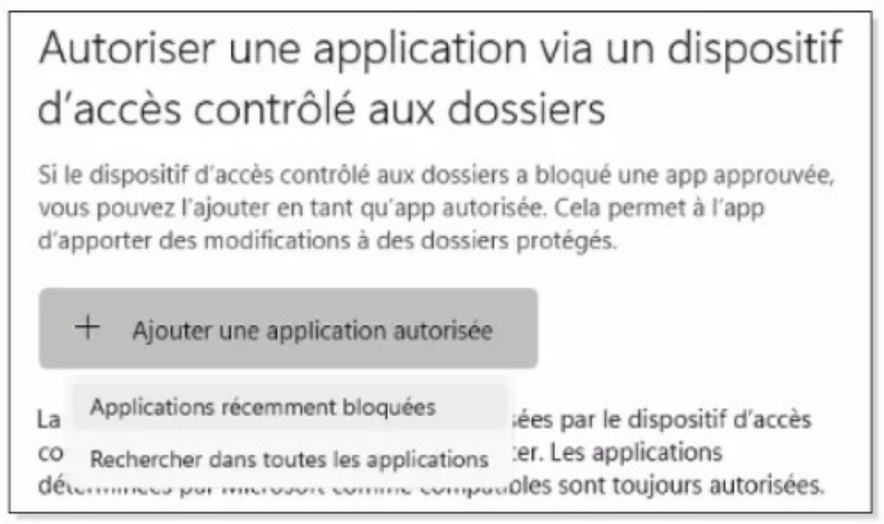
Pas question de perdre de précieuses données à cause d'un rançongiciel. Déjouez les attaques des pirates en activant les défenses antimalwares de votre ordinateur et en contrôlant l'accès à vos dossiers et applis.

1 DÉJOUEZ LES RANSOMWARES

Depuis le Bureau, cliquez sur la flèche de la barre des tâches pour afficher les icônes cachées, puis sur l'icône **Sécurité Windows**. Sélectionnez l'onglet **Protection contre les virus et les menaces** et, dans la section **Protection contre les ransomwares**, pointez sur **Gérer la protection les ransomwares**. Passez le curseur sous l'intitulé **Dispositif d'accès contrôlé aux dossiers** en position **Activé**. Les applications inconnues ou que vous n'avez pas encore approuvées ne peuvent désormais plus accéder aux dossiers Documents, Images, Vidéos, Musique et Favoris de votre compte Windows et de OneDrive, et encore moins les modifier.

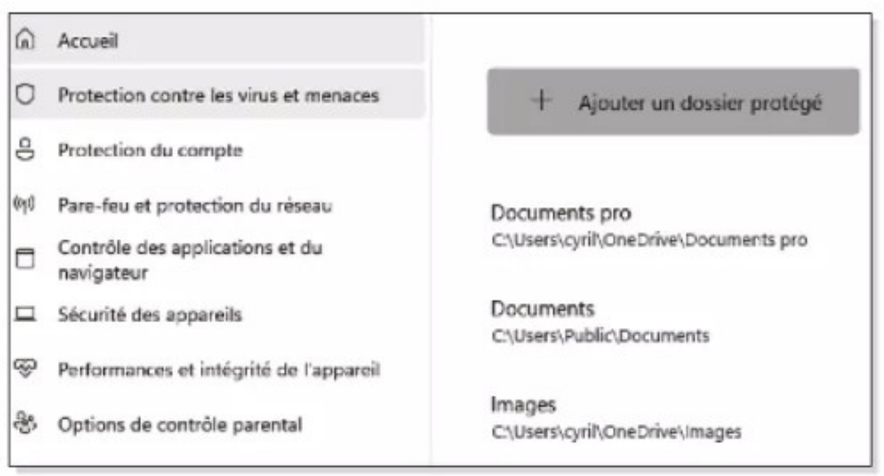
2 CRÉEZ UNE LISTE BLANCHE D'APPLICATIONS

Attention, ce type de protection empêche l'écriture d'une application tierce dans les dossiers sécurisés par Windows Defender. Le message d'erreur n'est pas toujours clair. Par exemple, un jeu peut refuser d'enregistrer une sauvegarde s'effectuant dans le dossier Mes documents sans prévenir qu'il n'a pas accès à cet emplacement. Sous l'intitulé **Dispositif d'accès contrôlé aux dossiers**, pointez sur **Autoriser une app via un dispositif d'accès contrôlé aux dossiers** puis sur le bouton **+ Ajouter une application autorisée**. Pointez sur **Applications récemment bloquées** pour redonner accès aux emplacements sécurisés à un logiciel. Si vous ne trouvez pas le programme dans la liste, utilisez la commande **Rechercher dans toutes les applications**.



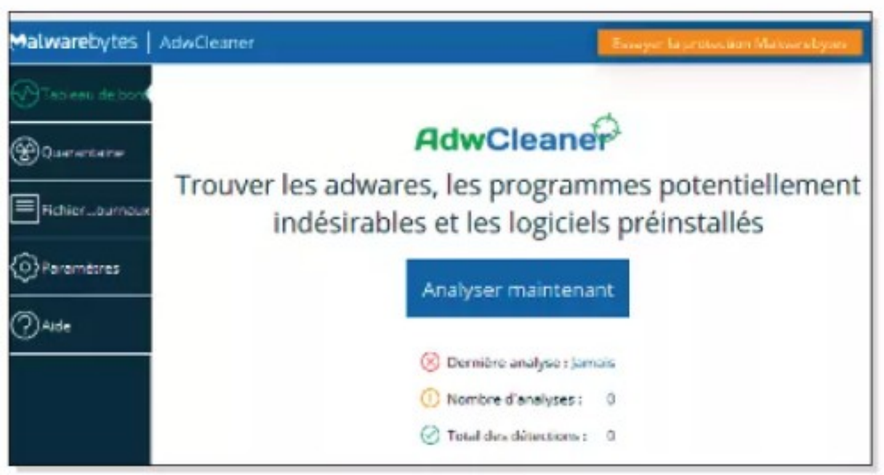
3 AJOUTEZ UN DOSSIER À PROTÉGER

Notez qu'il est possible de sélectionner le dossier C:\Programmes pour ajouter vos logiciels à la liste des applications autorisées à écrire dans les dossiers protégés. Vous pouvez compléter la liste des emplacements à sécuriser. Depuis la page **Protection contre les ransomwares**, cliquez cette fois sur **Dossiers protégés**, puis sur le bouton **+ Ajouter un dossier protégé**. Désignez le répertoire ou le disque où se trouvent des documents importants. Toutes ces précautions ne doivent pas empêcher d'effectuer une sauvegarde régulière des fichiers qui vous sont précieux. Si vous utilisez un disque dur externe, ne le laissez pas constamment connecté à l'ordinateur. Il doit être isolé afin de le protéger en cas d'attaque.



4 ANALYSEZ VOTRE SYSTÈME AVEC ADWCLEANER

Deux sécurités valant mieux qu'une, rendez-vous sur le site bit.ly/3XewBox et enclenchez le bouton **Téléchargement gratuit**. Le programme AdwCleaner ne nécessite pas d'installation. Lancez-le en effectuant un double-clic sur son fichier exécutable, puis pointez sur **Analyser maintenant**, de façon à lancer une recherche de logiciels malveillants sur l'ordinateur. Si un fichier dont l'innocuité ne fait aucun doute déclenche une alerte, on parle de faux positif. Cliquez alors sur **Paramètres**, **Exclusions**, **Ajoutez une exclusion** et désignez l'élément à exclure de l'analyse. Comme toute application portable, AdwCleaner peut être utilisé depuis une clé USB de dépannage.



DIFFICULTÉ **MODÉRÉE** TEMPS **15 MIN** DOMAINE **SÉCURITÉ**

RENFORCEZ LA PROTECTION DE VOTRE TÉLÉPHONE

Protéger son mobile n'est pas une option. C'est une nécessité absolue pour éviter d'exposer votre vie privée et vos données sensibles aux regards indiscrets. Démonstration.

1 VERROUILLEZ L'ACCÈS

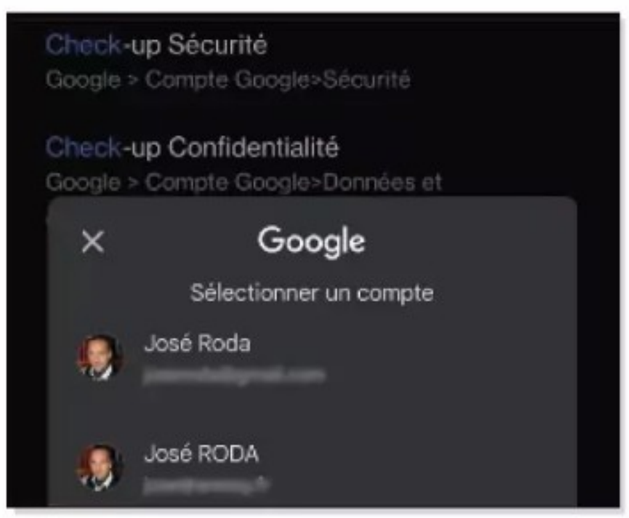
Vous aviez renoncé à l'écran de verrouillage de peur d'oublier votre code d'accès ? Alors optez pour d'autres modes de protection plus adaptés. Dans les paramètres d'Android, activez la rubrique **Mot de passe et sécurité**. Vous pouvez opter pour un dispositif d'identification biométrique comme la reconnaissance faciale, si votre mobile dispose d'une caméra compatible, ou le déverrouillage par empreinte digitale.

2 COMPARTIMENTEZ LES DONNÉES

Si vous avez l'habitude de prêter votre téléphone, ne prenez pas le risque que l'emprunteur consulte vos infos personnelles. Anticipez en définissant un profil au périmètre restreint, destiné à vos enfants ou amis, en plus de votre compte utilisateur. Dans **Paramètres**, **Utilisateurs et Comptes**, activez le mode **Plusieurs Utilisateurs**. Appuyez ensuite sur **Ajouter utilisateur** et configurez le nouvel espace.

3 LIMITEZ LA SAISIE SEMI-AUTO

Désactiver le mode de saisie automatique de Google oblige à solliciter davantage votre mémoire quand un mot de passe est exigé. En contrepartie, une personne mal intentionnée ne sera pas en mesure d'accéder à des services en ligne sensibles ou d'effectuer des achats à votre place. Dans le champ de recherche des paramètres d'Android, tapez le mot **semi-automatique**. Actionnez le curseur pour désactiver la fonction.

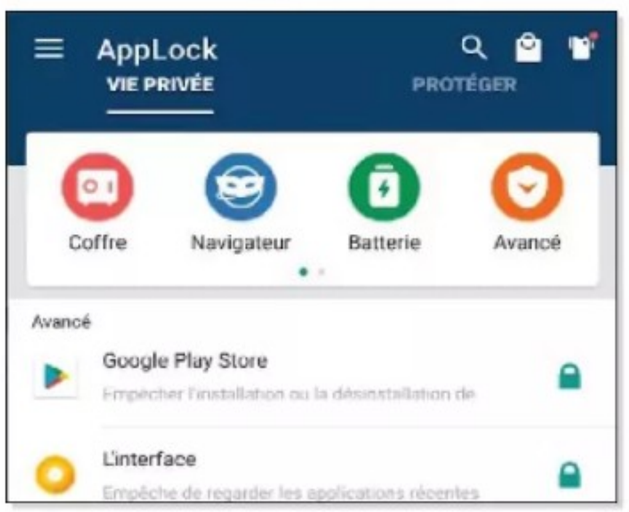


4 EFFECTUEZ UN CHECK-UP

Dans le champ de recherche des **Paramètres** d'Android, saisissez cette fois **check**. Parcourez les résultats et intéressez-vous aux commandes **Check-Up Sécurité** et **Check-Up confidentialité**. Exécutez-les au moins une fois par mois de façon à évaluer la santé globale du téléphone et de votre compte Google. En cas d'anomalie, Android vous suggère des actions de nature à combler les failles de sécurité.

5 ACTIVEZ LA GÉOLOCALISATION

L'outil de géolocalisation de Google ne sert pas seulement à savoir où se trouve votre téléphone en cas de perte ou de vol. Il permet de le verrouiller et d'en effacer le contenu à distance. Activez-le dans les **Paramètres**, en pointant sur **Localiser mon Appareil**, dans la section Google. En cas de besoin, connectez-vous à la page bit.ly/3Re35gf, entrez vos identifiants Google et prenez les mesures qui s'imposent.

6 BLOQUEZ LES APPLICATIONS

Téléchargez AppLock (bit.ly/3x687EP) sur le Play Store. Cette application conditionne l'accès aux applis et aux photos sensibles à la saisie d'un code. Définissez ce dernier, puis verrouillez les contenus de votre choix (réseaux sociaux, messagerie, etc.). Quelqu'un connaissant le code PIN de votre smartphone ne pourra donc pas afficher le contenu des applis.