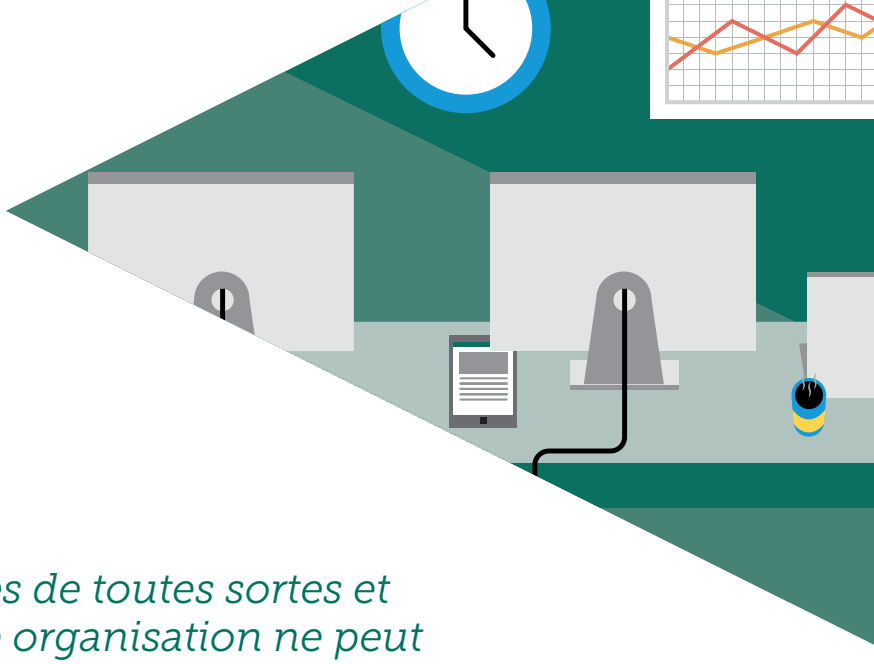
GUIDE PRATIQUE DE LA SÉCURITÉ INFORMATIQUE POUR LES PETITES ENTREPRISES

Comment s'assurer que votre entreprise dispose d'une protection informatique complète ?

#protectmybiz

KASPERSKY lab



Il existe des petites entreprises de toutes sortes et de toutes tailles. Mais aucune organisation ne peut se permettre d'ignorer la sécurité informatique, qu'il s'agisse d'une équipe travaillant dans un bureau, ou d'une personne travaillant à la maison. C'est un problème qui concerne tout le monde.

Si la cyber-criminalité fait souvent les gros titres, c'est généralement lorsqu'une grosse entreprise ou le gouvernement en est la victime. Mais les cas de moindre importance font souvent les plus grandes histoires.

Rien qu'en 2014, 143 millions de nouveaux cas de logiciels malveillants ont été détectés.[1] La majorité d'entre eux étaient dirigés contre des individus et des entreprises qui ne se considèrent pas comme des cibles potentielles.

En vérité, tout le monde peut être une cible. Rassurez-vous, il y a toujours une énorme différence entre être une cible et une victime.

Dans la plupart des cas, cela se résume simplement à une bonne préparation. C'est pourquoi nous avons réalisé ce guide : pour vous donner le savoir-faire afin de protéger votre entreprise.

? QU'EST-CE QU'UN LOGICIEL MALVEILLANT ?

Le terme logiciel malveillant se réfère aux programmes informatiques conçus dans un but malveillant. Ils attaquent généralement les appareils à l'insu de l'utilisateur. Kaspersky Lab est un leader mondial dans la détection des logiciels malveillants, ayant obtenu les meilleurs scores par rapport aux autres fournisseurs de sécurité.[2]

? POURQUOI AI-JE BESOIN D'UNE PROTECTION ?

Les cyber-criminels n'ont pas besoin de vider votre compte en banque pour avoir une incidence coûteuse sur votre entreprise. Les perturbations causées par les programmes malveillants peuvent interrompre votre productivité ou des flux de trésorerie, causant une série d'effets indésirables. Comme vous pouvez vous protéger contre ces éventualités avec des mesures relativement simples, vous serez rapidement à l'abri des soucis.

1. Tests AV
2. Étude des résultats de tests indépendants TOP 3 2014

VOTRE CHECKLIST DE SÉCURITÉ

LA PREMIÈRE ÉTAPE POUR SÉCURISER VOTRE ENTREPRISE CONSISTE À OBSERVER VOTRE FAÇON DE TRAVAILLER ET IDENTIFIER LES DOMAINES OÙ VOUS POURRIEZ RÉDUIRE LES RISQUES. EFFECTUEZ UN CONTRÔLE RAPIDE DE L'ÉTAT DE SANTÉ DE VOTRE SÉCURITÉ INFORMATIQUE :

PROTECTION CONTRE LES PROGRAMMES MALVEILLANTS ✔

Comme pour les assurances, lorsqu'il s'agit de produits qui protègent votre entreprise, vous voulez toujours le meilleur. Si vous n'avez pas encore de logiciel capable de protéger vos appareils contre les infections, vous devriez en faire une priorité.

Malheureusement, faire preuve de vigilance quand vous allez sur Internet ne suffit pas. Nous savons tous qu'il ne faut pas ouvrir de pièces jointes provenant d'expéditeurs inconnus ou télécharger des fichiers sur des sites suspects, mais bon nombre d'infections proviennent de sources dignes de confiance qui ont été compromises.

COMPORTEMENTS DE NAVIGATION ✔

Former votre personnel sur l'importance de leurs actions sur Internet peut vous éviter pas mal de soucis. Vos collaborateurs comprennent certainement qu'il y a certains types de sites sur lesquels ils ne doivent pas aller au travail. Mais s'ils utilisent également un appareil mobile (smartphone ou tablette) pour une utilisation personnelle, ils sont peut-être moins soucieux de la sécurité une fois qu'ils quittent vos locaux. Il est donc opportun de bloquer des sites inappropriés pour vous assurer qu'ils sont inaccessibles depuis les appareils mobiles que vous leur fournissez. Une meilleure prise de conscience générale à l'égard des menaces informatiques aidera aussi les employés à avoir une utilisation personnelle sécurisée.

DE NOMBREUSES INFECTIONS PROVIENNENT DE SOURCES DE CONFIANCE

? EN QUOI SUIS-JE CONCERNÉ ?

Vous n'avez jamais reçu un e-mail d'un ami ou d'un membre de votre famille contenant un lien intéressant qui, une fois ouvert, semblait suspect ? Dès que le logiciel malveillant a infecté un ordinateur, il peut agir à l'insu de l'utilisateur. Ne vous fiez donc pas toujours aux sources de confiance.

MOTS DE PASSE ✔

Les employés doivent également s'assurer qu'ils utilisent des mots de passe sécurisés et uniques qui mélangent des symboles, des chiffres et des lettres majuscules et minuscules. Les mots usuels peuvent être craqués par des programmes qui scannent des dictionnaires jusqu'à ce qu'ils trouvent le bon. Et même s'il est sécurisé, si un mot de passe compromis est utilisé à des fins multiples, il peut donner accès à de nombreux comptes.

MISES À JOUR ✔

Quatre nouveaux logiciels malveillants sont détectés chaque seconde.[3] Vous devez anticiper. Cela signifie qu'il faut utiliser des mises à jour automatiques de vos logiciels de sécurité et actualiser tous vos autres logiciels chaque fois que cela est possible en veillant à ce que tout le monde dans l'entreprise le fasse. Les programmes qui n'ont pas été mis à jour sont les premiers itinéraires utilisés par les cyber-criminels pour pirater les entreprises.

VEILLEZ À NE PAS COMMETTRE CES ERREURS CLASSIQUES :

1. Utiliser des mots de passe faciles à mémoriser mais faciles à deviner tels que 'mot de passe' ou ' 123456'
2. Utiliser votre adresse e-mail, votre nom ou d'autres données faciles à obtenir comme mot de passe
3. Définir des questions de rappel du mot de passe auxquelles un pirate pourrait répondre en cherchant un peu, comme le nom de jeune fille de votre mère
4. N'effectuer que de légères modifications évidentes aux mots de passe standard, comme ajouter un '1' à la fin
5. Utiliser des phrases courantes. Même les petites phrases comme « jetaime » sont faciles à deviner

Pour obtenir davantage de conseils sur la manière de définir des mots de passe difficile à pirater, consultez notre blog sur le sujet.

3 Tests AV

EN 2014

295,500

NOUVELLES MENACES DE LOGICIELS MALVEILLANTS POUR MOBILES[4]

SERVICES BANCAIRES ✔

Les cyber-criminels utilisent un certain nombre de méthodes pour obtenir vos informations financières : ils vous dirigent vers de fausses versions de sites de confiance ou utilisent des logiciels malveillants pour espionner votre activité. Vous devez prendre des mesures actives pour les arrêter.

Soyez attentif aux tentatives de phishing pendant lesquelles des escrocs usurpent l'identité de votre banque : utilisez toujours un navigateur sécurisé et vérifiez l'URL avant de saisir vos coordonnées sur un site. Il est également préférable d'éviter d'inclure ces informations dans des e-mails qui peuvent être consultés par des yeux malveillants.

APPAREILS MOBILES ✔

Comme le travail nomade fait maintenant partie de notre vie quotidienne, la cyber-criminalité est de plus en plus dirigée vers les appareils mobiles. En 2014, 295 500 nouveaux logiciels malveillants (spécifiquement conçus pour les smartphones et tablettes) ont été détectés chaque mois.[5] Même s'il est tout aussi important de protéger les téléphones et tablettes que les Mac et PC, seules 32 % des petites entreprises sont actuellement conscientes du risque que les appareils mobiles représentent.[6]

CHIFFREMENT ✔

Si des données sensibles sont stockées sur vos ordinateurs, elles doivent être chiffrées afin d'éviter les pertes, les vols et tout ce qui les rendrait inutilisables. Il est important de comprendre qu'en tant qu'entreprise, les informations que vous détenez sont précieuses et doivent être protégées.

? QU'EST-CE QUE LE PHISHING ?

Le phishing est l'usurpation d'identité d'une institution fiable par un cyber-criminel qui espère obtenir des informations telles que des mots de passe et informations de carte de crédit qu'il pourrait utiliser pour vous escroquer.

4 & 5 Selon Kaspersky Lab
6 Enquête 2014 sur les risques liés à sécurité informatique pour les entreprises

COMPRENDRE LES RISQUES

IL EST BIEN DE PARLER DE CYBER-SÉCURITÉ, MAIS POUR LA PLUPART D'ENTRE NOUS, CETTE RÉALITÉ EST PARFOIS DIFFICILE À COMPRENDRE. NOUS AVONS DONC ESSAYÉ DE LA SIMPLIFIER EN ILLUSTRANT QUELQUES SCÉNARIOS, LEURS CONSÉQUENCES ET COMMENT ILS POURRAIENT ÊTRE ÉVITÉS.

Une tasse de café qui coûte cher

Après avoir salué son dernier client de la journée, Thomas laisse à un de ses collègues le soin de fermer les locaux à clé. Il y a un café juste en face du bureau où il doit rencontrer un ami. Se souvenant qu'il doit effectuer un paiement à l'un de ses fournisseurs avant le lendemain, il décide de le faire avant d'oublier.

Il utilise son ordinateur portable pour se connecter au réseau wifi du café, se connecte ensuite au site Web de sa banque et effectue le transfert. Heureux de constater que son esprit est toujours vif, il se rassoit et profite de son café.

Lorsqu'il vérifie ensuite son compte bancaire, il s'aperçoit qu'il est vide. Pendant qu'il cherche à comprendre pourquoi, ses employés attendent leur paye.

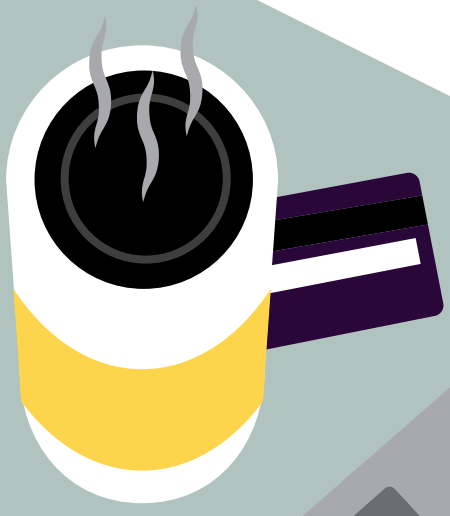
COMMENT CELA A-T-IL PU ARRIVER ?

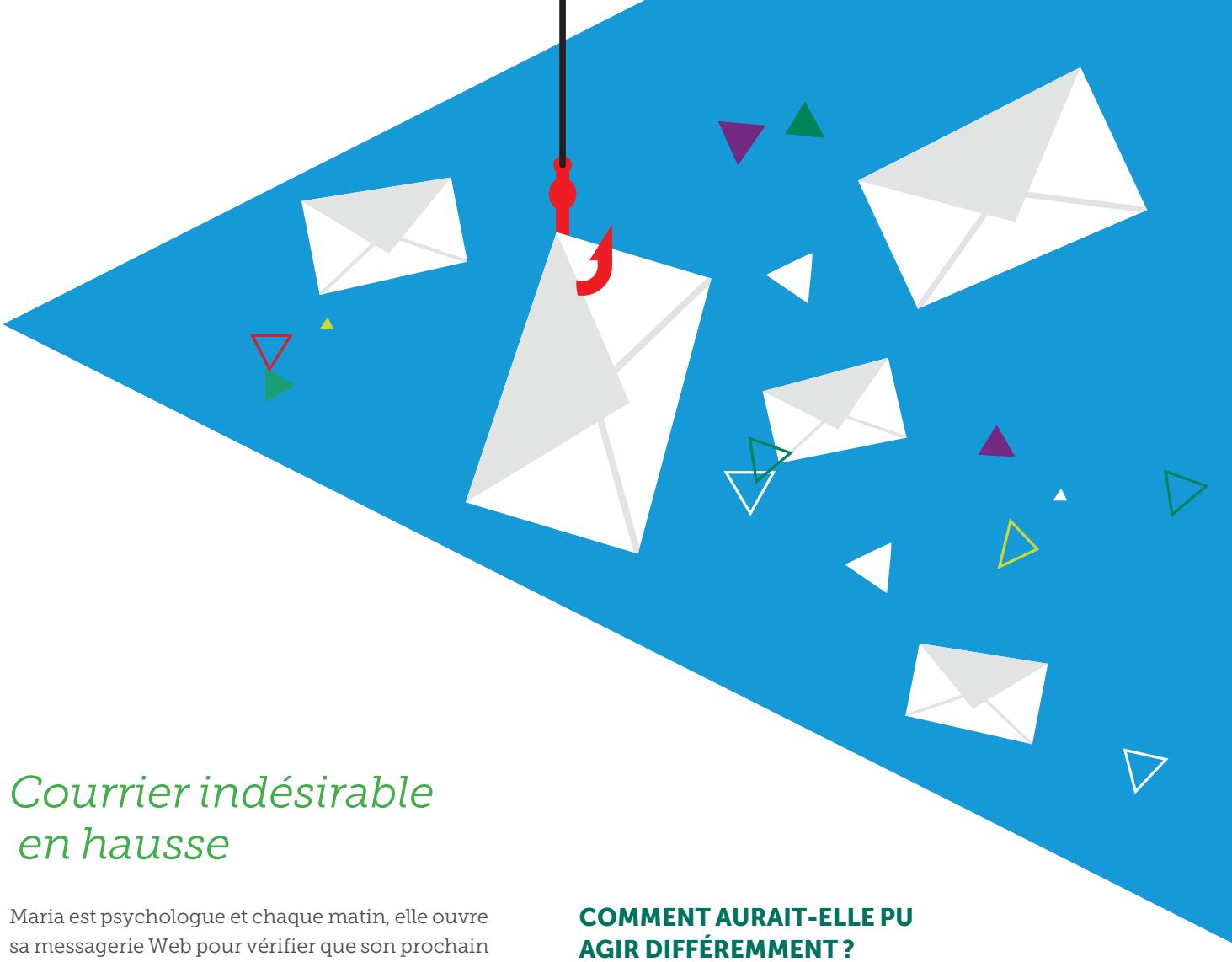
Malheureusement, sans aucune forme de protection contre les programmes malveillants, son ordinateur a été infecté par un logiciel d'enregistrement de frappe. Ceux qui ont lancé le programme ont reçu un enregistrement de toutes les informations qu'il a saisies. Et comme il utilisait un réseau wifi public non protégé, il y a également un risque que la transaction elle-même ait été interceptée.

QUE POUVAIT-IL FAIRE ?

Les transactions bancaires ne doivent être effectuées que sur des appareils équipés d'une protection contre les programmes malveillants avec un navigateur sécurisé. Avec la fonction Safe Money de Kaspersky Lab, Thomas aurait été en mesure de garantir sans nul doute possible que la transaction était sécurisée.

Il est intéressant de noter que, comme il utilisait un réseau public non sécurisé, les données qu'il était en train de transmettre ont pu être interceptées beaucoup plus rapidement qu'avec une connexion privée. Mais avec une fonction comme Safe Money, il aurait pu profiter de la commodité des services bancaires en ligne sans avoir à s'inquiéter.





Courrier indésirable en hausse

Maria est psychologue et chaque matin, elle ouvre sa messagerie Web pour vérifier que son prochain rendez-vous est confirmé. Dans sa boîte de réception, elle voit un message d'un réseau social qu'elle utilise lui demandant de mettre à jour son mot de passe pour le sécuriser. Elle clique sur le lien fourni, confirme son mot de passe existant (qui est identique) et remplace toutes les autres lettres par un astérisque.

Heureuse de savoir que son compte sera désormais plus difficile à pirater, elle retourne dans sa boîte de réception et oublie vite le tout...

... Jusqu'à ce qu'elle reçoive un message de chantage menaçant de publier les données des patients qu'elle suit en thérapie.

COMMENT CELA A-T-IL PU ARRIVER ?

Maria a été victime d'une escroquerie de phishing. Même si le site ressemblait exactement à celui qu'elle a visité des milliers de fois, il s'agissait d'une fausse copie. Ayant obtenu l'accès aux données de son profil, les maîtres chanteurs ont également découvert les détails de ses consultations. Ils ont essayé d'utiliser le même mot de passe que celui qu'ils lui ont volé pour pirater la messagerie de son travail. Et comme elle l'utilise pour les deux comptes, ils ont été en mesure de lire tous les messages et les fichiers joints, dont l'un était une liste complète de ses patients et de leurs coordonnées.

COMMENT AURAIT-ELLE PU AGIR DIFFÉREMMENT ?

Elle aurait dû d'abord savoir que les sites et organisations légaux ne demandent jamais vos données personnelles par e-mail. Une fois qu'elle a cliqué sur le lien, si elle avait eu un bon logiciel de sécurité, elle aurait été alertée du fait que le site était un faux.

Son autre erreur a été d'utiliser le même mot de passe dans le contexte professionnel et dans le contexte privé.

POURQUOI CHOISIR KASPERSKY LAB ?

NOUS NOUS SOMMES FIXÉS COMME MISSION D'APPORTER LA PROTECTION LA PLUS EFFICACE ET RÉACTIVE CONTRE LES CYBER-MENACES. DANS KASPERSKY SMALL OFFICE SECURITY, NOUS VOUS APPORTONS CETTE EXPERTISE DANS UNE SOLUTION AUSSI PRATIQUE QUE CONVIVIALE. VOUS POUVEZ VOUS CONCENTRER SUR CE QUE VOUS FAITES LE MIEUX : GÉRER VOTRE ENTREPRISE.

Nous comprenons que, lorsqu'il s'agit de cyber-sécurité, les petites entreprises sont dans une position singulière. Elles font face aux mêmes menaces que les grandes entreprises et partagent les mêmes vulnérabilités que les particuliers. Nous pensons que cette position unique mérite sa propre approche de la sécurité.

Le simple usage d'un produit grand public comme solution pour les petites entreprises n'est pas suffisant. Par exemple, il n'offre aucune protection pour les serveurs, mais de nombreuses petites entreprises en utilisent un ou prévoient d'en utiliser. Contrairement aux particuliers, les entreprises ont besoin de protéger plusieurs appareils facilement.

Cependant, l'utilisation de solutions destinées aux grandes entreprises ne fonctionne pas non plus. Les petites entreprises ne disposent pas d'équipes informatiques dédiées ni du temps pour s'attaquer à un logiciel complexe conçu pour des spécialistes.

Kaspersky Small Office Security a été conçu pour être complet sans être complexe afin que vous puissiez rester serein, sans que la sécurité ne vienne ponctionner vos ressources. Cette solution ne vous ralentit pas et couvre un large éventail d'appareils, vous assurant une protection complète quelle que soit l'évolution de votre entreprise.

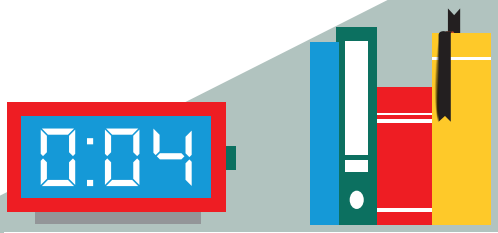
? PUIS-JE ME PROTÉGER GRATUITEMENT ?

Bien que des solutions de sécurité gratuites soient disponibles, elles n'offrent tout simplement pas de protection complète. En fait, elles laissent délibérément de la place à l'amélioration. C'est la manière dont elles encouragent les utilisateurs à passer à une version payante.

Lorsque votre entreprise est en jeu, votre protection doit être la meilleure possible, tout le temps.

COMMENT AGIR ?

MAINTENANT QUE NOUS AVONS IDENTIFIÉ LES ZONES QUE VOUS DEVEZ EXAMINER DANS LE CADRE DE VOTRE POLITIQUE DE SÉCURITÉ, IL EST TEMPS D'ENVISAGER COMMENT, AVEC L'AIDE D'UNE SOLUTION SUR MESURE, VOUS POUVEZ LA METTRE EN ŒUVRE.



MISES À JOUR RÉGULIÈRES

Lorsqu'il s'agit de Kaspersky Small Office Security, vous ne devez pas vous inquiéter. Nous mettons à jour automatiquement votre protection en temps réel pour vous tenir à l'écart des nouvelles menaces au fur et à mesure de leur apparition.

RENFORCEMENT DES MOTS DE PASSE

Simplifiez cette tâche pour vos employés en utilisant Kaspersky Password Manager. Il génère automatiquement des mots de passe sûrs et les stocke dans une base de données chiffrée. Vous n'avez plus qu'à mémoriser un seul mot de passe et votre sécurité est renforcée.

CHIFFREMENT ET SAUVEGARDE DES DONNÉES SENSIBLES/ CRITIQUES

Avec Kaspersky Small Office Security, il est facile de stocker vos informations critiques en coffres-forts sécurisés. La fonction de restauration signifie que même si vos ordinateurs ou serveurs tombent en panne, les données vitales ne sont pas perdues.

PROTECTION POUR TOUS VOS APPAREILS

Kaspersky Small Office Security offre une protection pour les tablettes et smartphones supportés. Et si les appareils sont perdus ou volés, elle peut vous aider à les localiser et à effacer à distance toutes les informations sensibles.

BLOCAGE DES PIRATES

Notre fonction Safe Money primée peut être activée en quelques clics et permet une navigation en toute sécurité. En l'utilisant pour vérifier que les sites avec lesquels vous interagissez ne sont pas compromis, vous pouvez instantanément éviter l'exploitation des failles. Pendant ce temps, nos fonctions de pare-feu et de protection contre les programmes malveillants et le courrier indésirable tiennent les criminels à l'écart quand vous allez sur internet.

PROTÉGEZ VOTRE ENTREPRISE MAINTENANT.

Développé pour répondre aux exigences uniques des petites entreprises, Kaspersky Small Office Security combine un niveau de protection élevé avec une grande simplicité d'utilisation pour les entreprises comme la vôtre.

Visitez **kaspersky.fr/protege-mon-entreprise** et découvrez comment Kaspersky Small Office Security peut protéger votre entreprise.

PROTÉGEZ VOTRE ENTREPRISE MAINTENANT

RETROUVEZ-NOUS SUR LES RÉSEAUX SOCIAUX

#protectmybiz

Visionnez nos vidéos sur YouTube

Rejoignez nos fans sur Facebook

Découvrez le blog d'Eugène Kaspersky

Suivez-nous sur Twitter

Retrouvez-nous sur LinkedIn

Plus d'informations sur kaspersky.fr/protege-mon-entreprise

À PROPOS DE KASPERSKY LAB

Kaspersky Lab est le plus grand éditeur privé mondial de solutions de protection des terminaux. La société fait partie des quatre principaux éditeurs mondiaux de solutions de sécurité pour utilisateurs de terminaux informatiques*. Depuis plus de 17 ans, Kaspersky Lab fait figure de précurseur dans le domaine de la sécurité informatique, fournissant des solutions de sécurité numérique efficaces aux grandes entreprises, PME et particuliers. Kaspersky Lab, dont la holding est enregistrée au Royaume-Uni, opère actuellement dans près de 200 pays et territoires du monde entier et offre une protection à plus de 400 millions d'utilisateurs. Plus d'informations sur www.kaspersky.com.

* L'entreprise est classée quatrième fournisseur mondial de solution de sécurité des terminaux, en termes de chiffre d'affaires, par IDC en 2013. Ce classement a été publié dans le rapport IDC « Worldwide Endpoint Security 2014-2018 Forecast and 2013 Vendor Shares » (Sécurité des terminaux dans le monde : prévisions pour 2014-2018 et parts de marché des fournisseurs en 2013), document numéro 250210, août 2014. Ce rapport classait les éditeurs de logiciels selon leurs revenus provenant des ventes de solutions de sécurité des terminaux en 2013.