6 CONSEILS pour un télétravail en toute sécurité

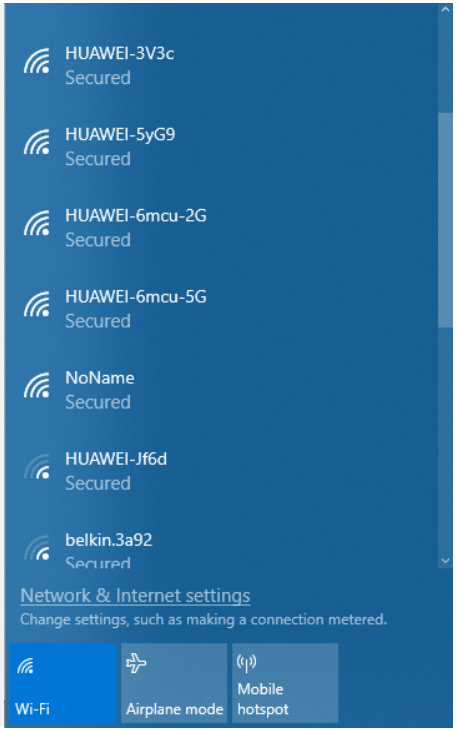
En cette période de pandémie de coronavirus, nombreux sont les employés à devoir travailler de chez eux et peut-être en faites-vous d'ailleurs partie ! Voici donc quelques conseils et bonnes pratiques en matière de cybersécurité pour vous aider à vous défendre en cas de cyberattaques. Ces quelques étapes peuvent vraiment faire la différence et sécuriser davantage votre environnement informatique et digital lorsque vous travaillez de chez vous.

1 Vérifiez les paramètres de votre routeur domestique et modifiez ceux ayant été établis par défaut

Lorsque vous travaillez de chez vous, l'ensemble de votre trafic web passe par votre routeur domestique. Les cybercriminels peuvent tenter de pirater ce dernier, de faire main basse sur ce qui transite depuis votre Wi-Fi, voire même d'accéder à votre réseau. Si vous n'avez donc pas encore examiné les différentes options de configuration de votre routeur à la maison, nous vous conseillons de vous y atteler dès à présent et surtout avant que votre réseau et vos appareils connectés ne soient véritablement menacés.

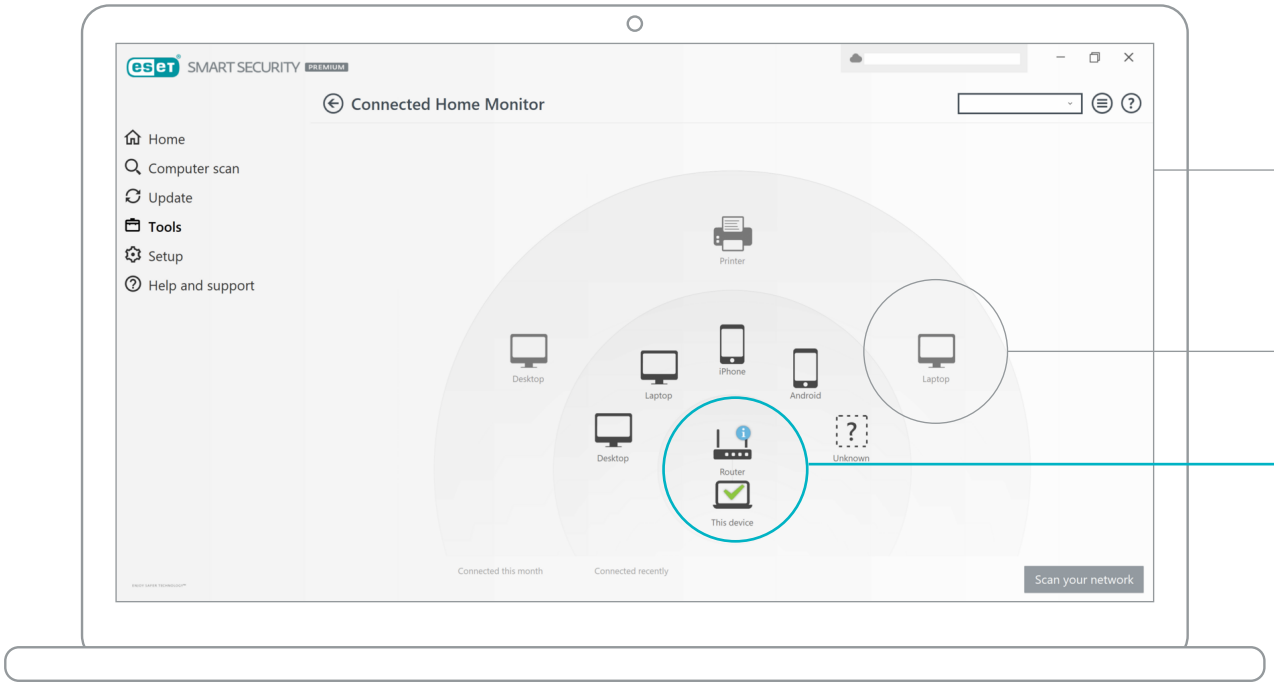
Sécurisez votre réseau domestique en 4 étapes très simples

1. Connectez-vous sur votre réseau domestique
2. Accédez au panneau de configuration en tapant l'adresse IP de votre routeur dans votre navigateur, par exemple : 192.168.1.1 (consultez le manuel de votre appareil pour connaître son adresse exacte)
3. Assurez-vous de bien modifier les noms et mots de passe utilisés par défaut et associés à votre routeur
4. N'oubliez pas également de changer votre SSID (Service Set Identifier), à savoir le nom de votre réseau, qui sinon risque de vite devenir une information utile pour un cybercriminel.



2 Analysez votre réseau domestique et démasquez les appareils indésirables

Utilisez des outils fiables d'analyse afin de détecter les appareils indésirables présents sur votre réseau domestique. Par exemple, notre logiciel ESET Smart Security Premium est doté d'une fonctionnalité d'analyse, Connected Home Monitor, qui vous indiquera si des voisins indélicats se sont connectés sur votre Wi-Fi à votre insu. **Modifiez votre mot de passe et faites le ménage sur votre réseau !**



VOICI L'OUTIL D'ANALYSE D'ESET, LE CONNECTED HOME MONITOR,

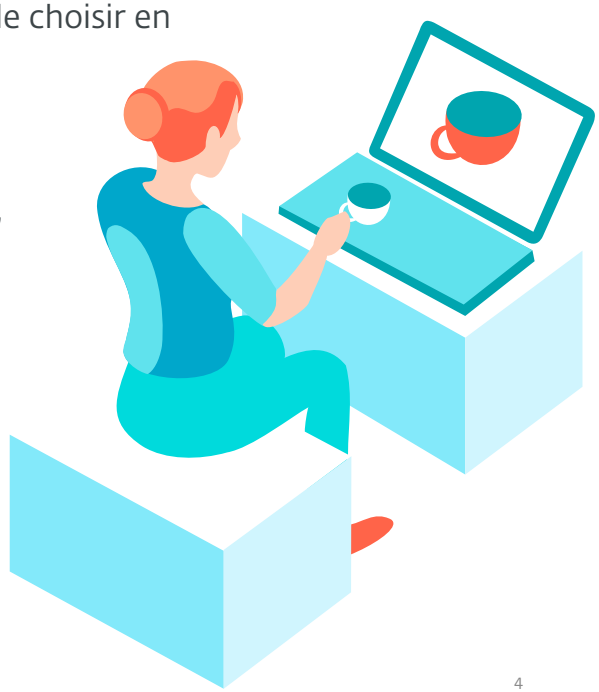
QUI DÉTECTE LES APPAREILS INDÉSIRABLES.

CETTE FONCTION VOUS AIDE À GARDER VOTRE RÉSEAU EN SÉCURITÉ. MODIFIEZ VOTRE MOT DE PASSE RÉSEAU AFIN DE VOUS PROTÉGER DAVANTAGE.

3 Mettez à jour le firmware (micrologiciel) de votre routeur domestique — ou bien cessez d'utiliser votre ancien routeur

Il est essentiel de vous assurer que le firmware de votre routeur est toujours mis à jour vers la dernière version disponible fournie par le fabricant. Les chercheurs ESET ont d'ailleurs récemment découvert la vulnérabilité KrØØk, laquelle aurait infecté des milliards de puces wi-fi intégrées dans des routeurs, entre autres appareils. **Alors si vous utilisez un vieux routeur, il est vraiment temps d'en changer !**

Dans le cas où vous souhaiteriez investir dans un nouveau routeur, assurez-vous de le choisir en fonction de ses options pour améliorer votre sécurité. Certains d'entre eux, comme les modèles de chez Gryphon, intègrent une option threat intelligence conçue par ESET. Celle-ci permet de détecter et de bloquer les malwares, les sites de hameçonnage ainsi que d'autres menaces présentes au niveau du réseau, pour chaque appareil connecté au routeur de votre maison.



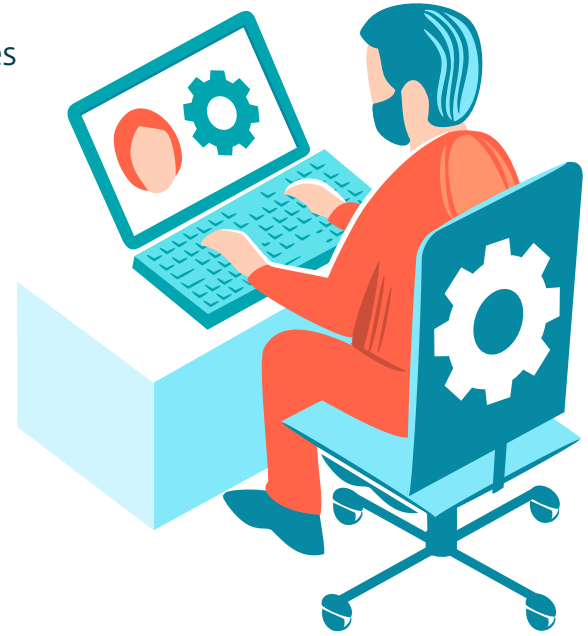
CONSEIL À DESTINATION DES UTILISATEURS AVANCÉS

La plupart des "Internet Routers of Things" actuels vous permettent de créer différents réseaux pour des objectifs tout aussi variés. Une pratique efficace consiste à utiliser cette fonction pour concevoir des réseaux séparés et ainsi prendre le moins de risques possible lorsque vous utilisez vos appareils les plus sensibles.

4 Utilisez un réseau privé virtuel (VPN) pour chiffrer vos communications

L'utilisation d'un VPN permet de créer un "tunnel" sécurisé pour vos communications établies avec l'intranet de l'entreprise.

Avec l'aide d'un VPN, les paquets de données qui composent les communications sont ainsi gardés à l'abri des regards indiscrets et ce même lorsque vous naviguez dans les profondeurs d'Internet. Le déchiffrement n'est alors possible qu'en fin de tunnel, c'est-à-dire directement sur votre ordinateur ou sur le réseau de la société. Si vous avez un département informatique, l'équipe en charge pourra vous conseiller sur l'application à télécharger sur votre appareil personnel puis vous communiquera des informations d'identification VPN, toujours dans l'optique d'apporter une solution cohérente à votre situation.



CONSEIL À DESTINATION DES UTILISATEURS AVANCÉS

Si vous n'avez pas de service informatique, vous devrez peut-être configurer vous-même vos connexions VPN. Rassurez-vous : c'est moins compliqué que ça n'en a l'air. Certains routeurs professionnels ainsi que d'autres plus petits (souvent destinés au télétravail ou aux PME) possèdent déjà une fonctionnalité VPN, ce qui est un vrai plus pour le budget. Il est donc tout à fait possible que vous ayez déjà un appareil de ce type, il vous reste ensuite juste à le paramétrer !

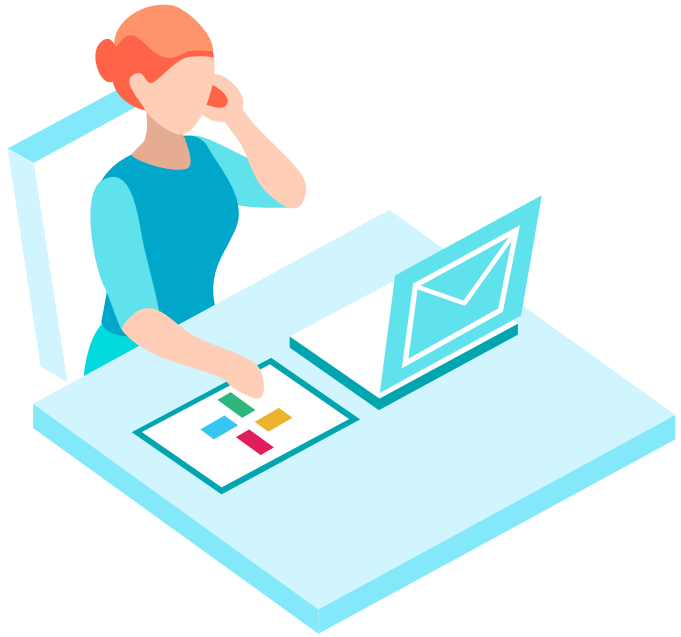
5 Si vous le pouvez, utilisez la double authentification (2FA)

Les employés en télétravail utilisant des technologies distantes telles qu'un Remote Desktop Protocol (RDP) peuvent plus facilement être attaqués si une politique de sécurité et des options de protection ne sont pas mises en place. Les cybercriminels spécialisés dans les menaces RDP **utilisent en général l'ingénierie sociale pour obtenir les mots de passe des utilisateurs,** ou usent des attaques dites par force_brute. En d'autres termes, la réussite de ces assauts contre les RDP peut provenir d'une mauvaise gestion du processus d'authentification ou d'un hameçonnage sournois, entre autres facteurs.

La protection en deux étapes relève de l'authentification multifacteur (MFA) qui exige de l'employé un code à usage unique délivré depuis une application d'authentification (l'option la plus sécurisée) ou à l'aide d'un SMS, tout ceci en plus de l'identifiant et du mot de passe habituels. Même si un pirate met la main sur le mot de passe, la solution 2FA mise en place empêchera tout accès non autorisé.

6 Suivez des formations en cybersécurité et éduquez-vous

Une formation pour mieux se sensibiliser à la cybersécurité devrait être un prérequis annuel pour chaque employé. Pourquoi ne pas commencer dès à présent ? D'autant que vous avez déjà intégré le télétravail à votre routine professionnelle ! En étant à distance, la tentation est plus grande de vouloir cliquer sur certains liens extérieurs à votre travail, en particulier lorsque ceux-ci traitent d'actualités ou de divertissements. En effet, de nombreuses arnaques au sujet du Covid-19 ont déjà été détectées. Ce qui peut prendre la forme d'un article traitant d'un potentiel vaccin peut finalement cacher des téléchargements dangereux ou simplement de fausses informations.



CONSEIL À DESTINATION DES UTILISATEURS AVANCÉS

Notre équipe de chercheurs chez ESET publie régulièrement ses dernières découvertes sur notre compte TWITTER notamment au sujet des nouvelles menaces détectées :

https://twitter.com/ESETresearch

Prenez soin de vous et restez protégé(s) !

Sécurisez vos précieux appareils personnels en installant ESET Internet Security dès maintenant et payez plus tard grâce à notre essai gratuit à durée prolongée !

EN SAVOIR PLUS