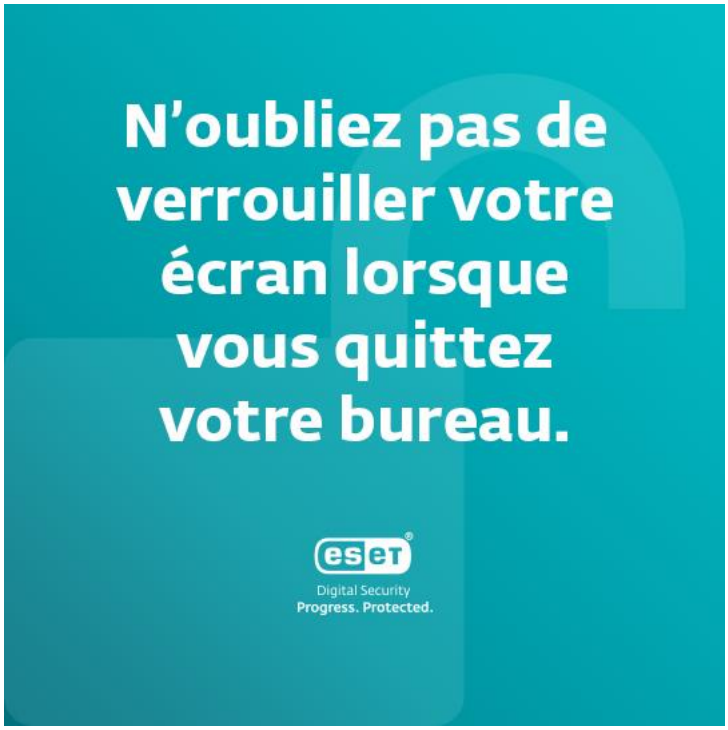
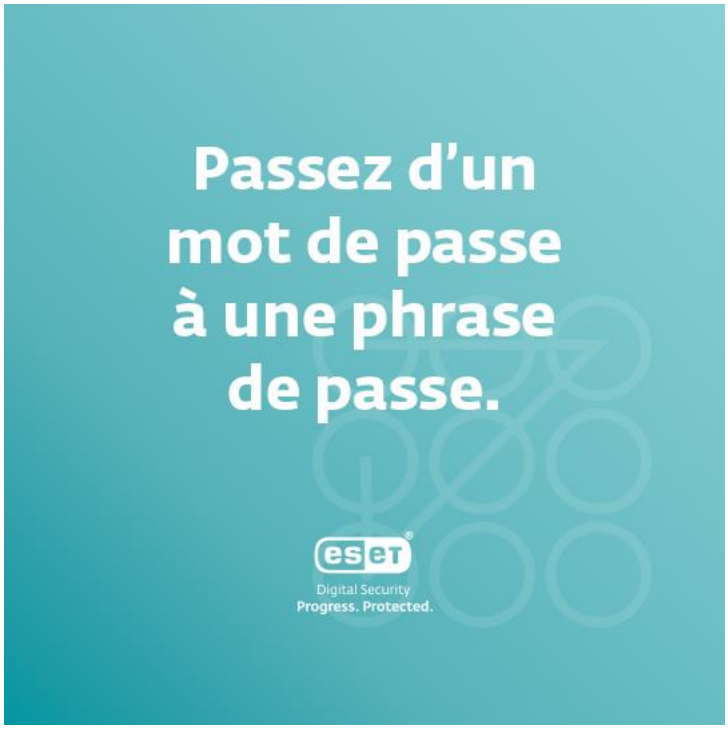


N’oubliez pas de verrouiller votre écran lorsque vous quittez votre bureau.

Pendant que certains profiteraient de l’occasion de vous surprendre en envoyant un email amusant à partir de votre compte, d’autres pourraient rechercher des données et les utiliser à mauvais escient. Protégez les données sensibles de votre entreprise en verrouillant systématiquement votre écran lorsque vous laissez votre ordinateur sans surveillance. Voici les raccourcis que vous pouvez utiliser pour verrouiller immédiatement votre écran.

- Sur Mac, appuyez sur les touches Contrôle + Commande + Q
- Sur PC, appuyez sur les touches Ctrl + Alt + Suppr, puis cliquez sur VERROUILLER



Passez d'un mot de passe à une phrase de passe.

Un bon mot de passe devrait être facile à retenir mais difficile à deviner. Plus il est long, mieux c'est. Le moyen le plus simple d'y parvenir est de transformer votre mot de passe en une phrase de passe. Comment créer une bonne phrase de passe ?

1. Idéalement, un bon mot de passe ou une bonne phrase de passe devrait être composé d'une combinaison de lettres majuscules et minuscules, de chiffres et de caractères spéciaux.
2. Incluez des informations que peu de gens connaissent, comme l'ancien surnom qui vous était donné quand vous étiez enfant, votre film préféré, ou une blague qui n'est drôle que pour vous.
3. Évitez les informations faciles à trouver, telles que le nom de vos animaux domestiques ou votre date de naissance.
4. Remplacez certains mots ou lettres par des chiffres et des symboles. Au lieu de « quelqu'un », essayez « kElqu_1 »
5. Ajoutez quelque chose d'aléatoire. Si vous choisissez, par exemple, une phrase tirée d'un film ou des paroles d'une chanson, quelqu'un l'a probablement déjà fait, ce qui rend le mot de passe plus facile à craquer. Essayez d'ajouter un élément sans rapport avec le sujet et qui n'a de sens que pour vous. Exemple :

   Changez « Décembre est le meilleur mois. » en « 9Decem8re-3st_LE-me1yeurM0A! »

Utilisez un mot de passe unique pour chacun de vos comptes.

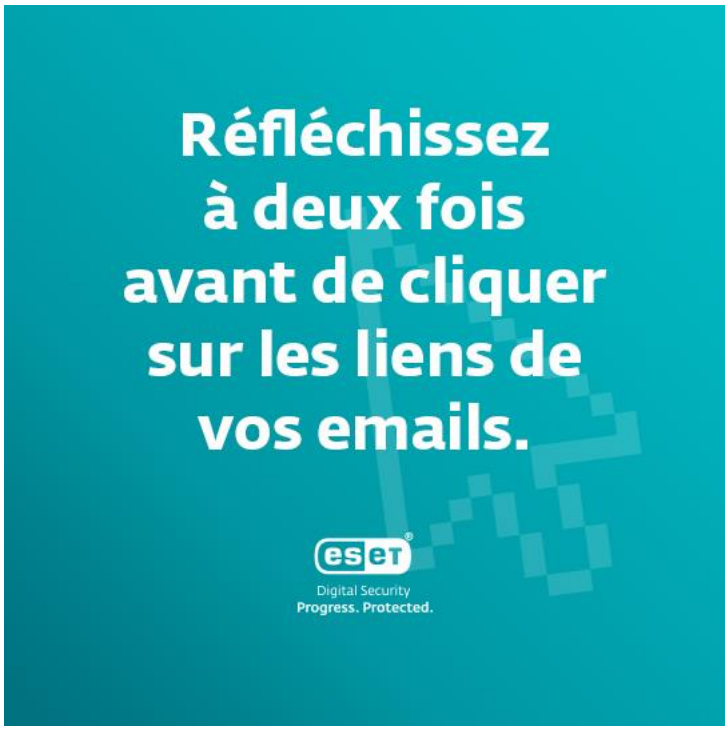
Vous pensez peut-être qu'il importe peu que quelqu'un pirate le mot de passe de votre compte client IKEA. Vous avez peut-être raison, tant que vous n'utilisez pas ce même mot de passe pour d'autres comptes, y compris ceux que vous utilisez pour votre travail. Lorsque vous réutilisez le même mot de passe sur tous vos comptes, il est peut-être plus facile à retenir, mais il n'est absolument pas sécurisé. Prenez le temps d'examiner vos comptes et de modifier vos identifiants de connexion afin d'en utiliser un différent pour chaque compte.

Utilisez un gestionnaire de mots de passe.

Si vous utilisez des phrases de passe sécurisées ou un mot de passe unique pour chacun de vos comptes, il peut être difficile de se souvenir de tous vos identifiants. Les gestionnaires de mots de passe sont conçus pour vous aider. En stockant vos ID dans un gestionnaire de mots de passe, vous n'avez à retenir qu'un seul mot de passe tout en maintenant un niveau élevé de sécurité. Idéalement, vous pouvez également activer l'authentification multifacteur (MFA), qui améliore la protection du gestionnaire de mots de passe. Certains d'entre eux offrent également des fonctions spéciales, comme le stockage de documents confidentiels. Votre service informatique peut vous aider à choisir et installer un gestionnaire de mots de passe sûr et facile à utiliser.

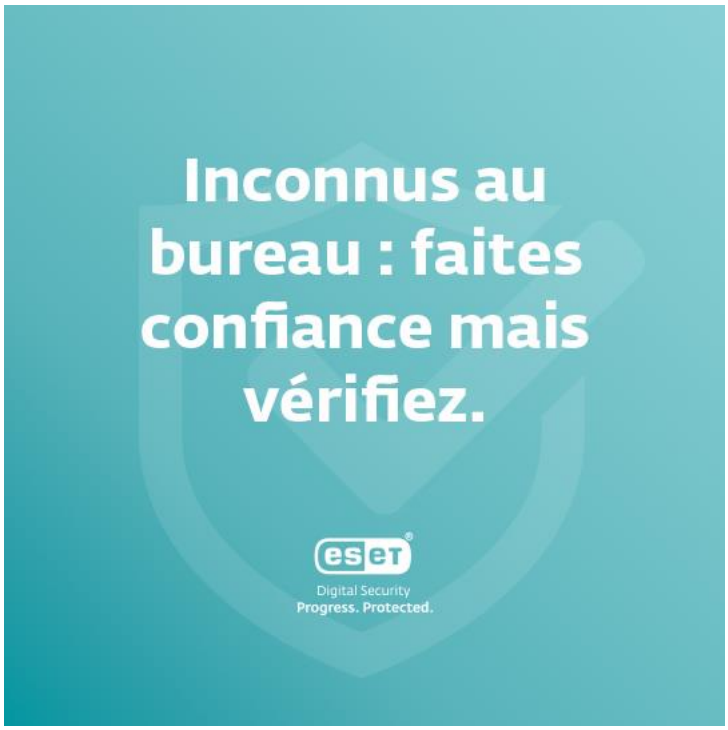
N’oubliez pas de consulter votre spécialiste informatique pour toute nouvelle application.

Vous voulez installer une nouvelle application sur votre appareil professionnel ? Consultez toujours votre équipe informatique. Elle devrait déterminer si l’application est sûre, en se basant par exemple sur la manière dont elle traite les données, les autorisations requises, ou les impacts sur les clients lorsque le fonctionnement de l’application est interrompu. Votre spécialiste informatique peut vous expliquer le fonctionnement de l’application et la manière de l’utiliser sans risque afin de protéger votre sécurité digitale et celle de l’entreprise.



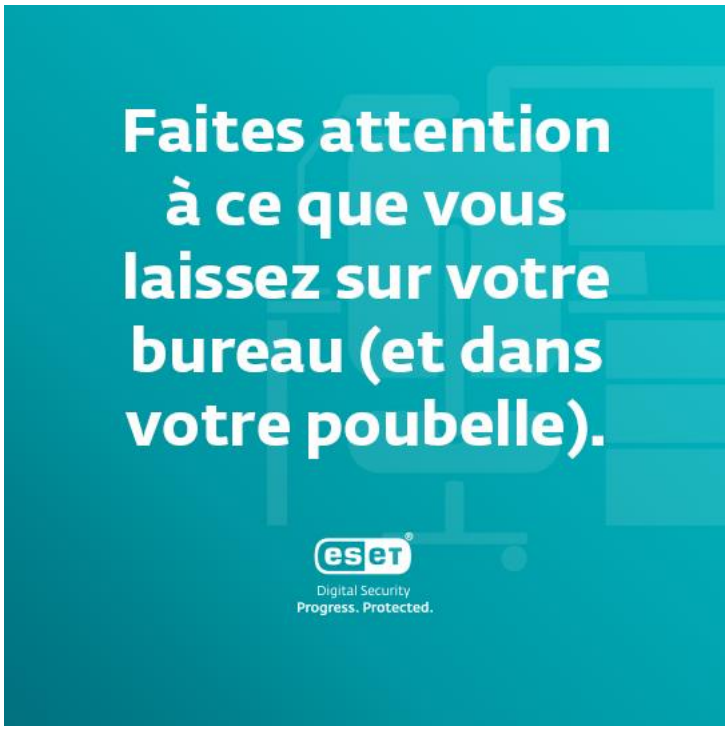
Réfléchissez à deux fois avant de cliquer sur les liens de vos emails.

Apprenez à reconnaître les tentatives d'hameçonnage et les tactiques utilisées par les cybercriminels pour vous attirer dans leurs pièges. Retrouvez quelques exemples et conseils ici. N'oubliez pas les éléments qui devraient vous mettre la puce à l'oreille pour identifier un email d'hameçonnage : salutation générique, fautes de grammaire, URL ou objet qui ne correspond pas au corps du message ou au sujet, sentiment d'urgence et obligation d'agir rapidement. Les internautes se font souvent piéger par des emails d'hameçonnage parce qu'ils agissent sous pression. Prenez le temps de lire prudemment vos emails et rappelez-vous que l'ouverture du message en lui-même est généralement sans danger. La menace éventuelle réside dans les pièces jointes et les liens inconnus, mais également dans les images incluses dans le message, qui peuvent permettre à l'attaquant de deviner votre localisation, votre appareil, votre système d'exploitation, etc. Il peut ensuite utiliser ces informations pour vous attaquer dans un second temps. Il est donc judicieux de désactiver le chargement automatique des images. Si vous repérez une tentative d'hameçonnage, alertez toujours votre service informatique.



Inconnus au bureau : faites confiance mais vérifiez.

Chaque fois que vous voyez une personne inconnue se promener dans les locaux de votre entreprise comme si elle était perdue, demandez-lui si elle a besoin de votre aide. Si elle vous semble suspecte, n'hésitez pas à la signaler à la sécurité. Comme pour d'autres domaines, il vaut mieux être sûr que de devoir faire face à une faille de sécurité en raison d'un intrus malveillant. Ce scénario vous semble irréaliste ? Lisez le récit de Jake Moore, un expert en cybersécurité qui s'est infiltré dans une entreprise et l'a piratée parce que les employés n'étaient pas assez vigilants.



Faites attention à ce que vous laissez sur votre bureau (et dans votre poubelle).

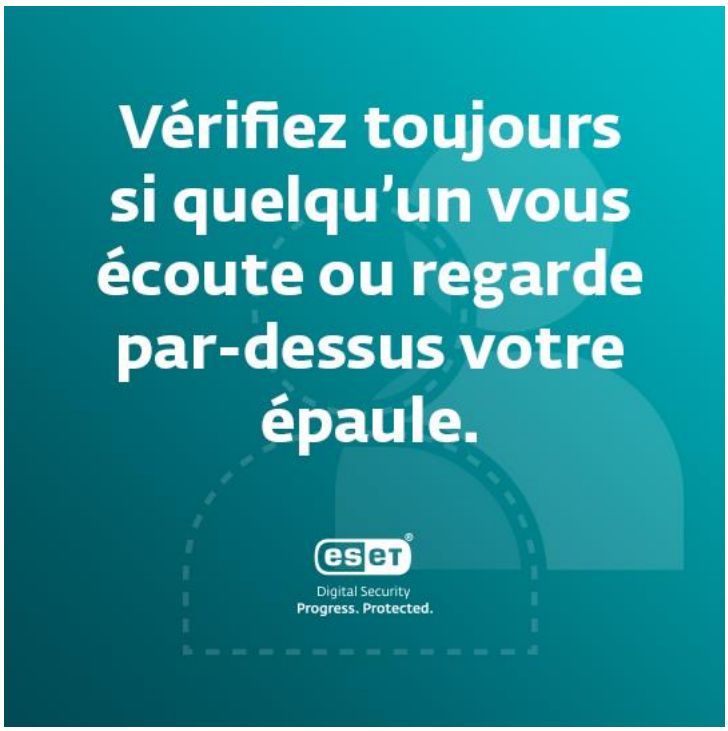
Nous avons aujourd'hui tendance à nous concentrer sur les données numériques plus que sur les documents physiques. Pourtant, si ceux-ci devaient quitter le lieu de travail et tomber dans les mains d'un inconnu, cela pourrait mettre votre entreprise en danger. Afin d'éviter cette situation, assurez-vous de détruire les documents confidentiels avant de les jeter. N'oubliez pas de vérifier également ce qui se trouve sur votre bureau. Comporte-t-il des documents que personne ne devrait lire ? Ou des notes importantes que vous ne voulez pas partager ? Mieux vaut les mettre dans une armoire verrouillée.

Évitez de vous connecter à des réseaux Wifi publics.

Les lieux dotés d'une connexion Wifi publique sont tentants, non seulement pour vous... mais aussi - hélas - pour les cybercriminels. Cela peut se traduire par des systèmes Wifi publics infectés par des malwares (via le routeur), par de fausses connexions Wifi publiques mises en place par des pirates, ou par des attaques dites « Man-in-the-Middle » (MitM) utilisées par les cybercriminels pour s'insérer entre vous et le point d'accès, et collecter vos données. Si vous devez vraiment vous connecter à du Wifi public, utilisez toujours votre VPN et ne consultez pas de sites qui vous demandent de saisir vos identifiants de connexion, comme les services bancaires sur Internet.

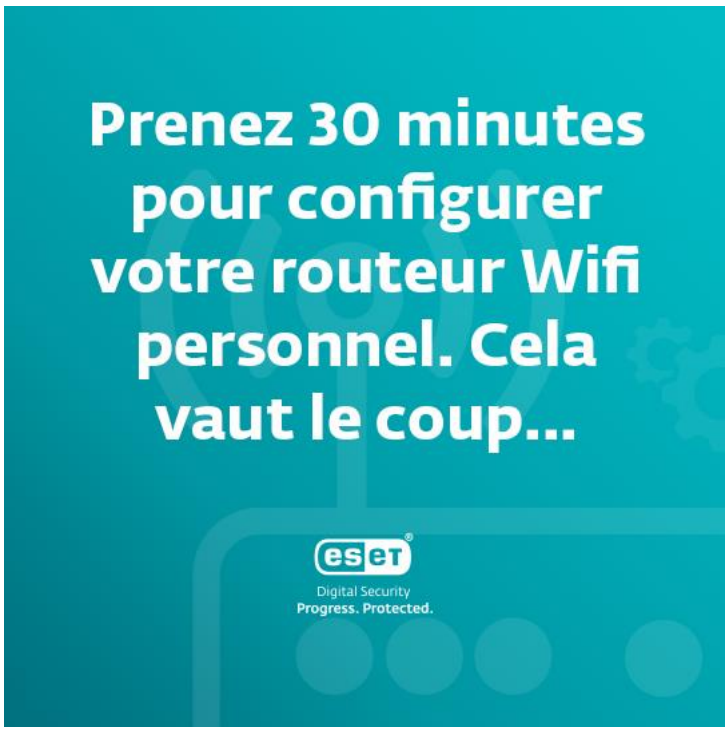
Pendant les conférences vidéo et le partage d'écran, ne montrez que ce qui est nécessaire pour l'appel.

Pour beaucoup, les conférences vidéo sont devenues une partie incontournable de leur travail. Mais tout comme vous le feriez en face-à-face, vous devez suivre certaines règles pour éviter tout risque. Si vous devez partager votre écran, veillez à ne montrer que les fenêtres qui doivent l'être et assurez-vous qu'il n'y ait pas de documents privés en arrière-plan. Il en va de même pour votre environnement. Si vous le pouvez, masquez votre arrière-plan et vérifiez toujours s'il n'y a pas quelque chose derrière vous qui ne devrait pas être partagé, comme un tableau blanc avec les notes d'une réunion interne.



Vérifiez toujours si quelqu'un vous écoute ou regarde par-dessus votre épaule.

Vous devez vous connecter à vos comptes professionnels dans le bus ? Ou passer un appel téléphonique professionnel dans un café, ou même dans votre propre jardin ? N'oubliez pas que les personnes à proximité peuvent en profiter pour scruter votre écran pour ensuite accéder à vos comptes ou entendre des informations confidentielles. Lorsque vous êtes dans un lieu public, utilisez une autorisation biométrique, telle que Touch ID. Lorsque vous travaillez à distance, sachez que toute personne extérieure à l'entreprise peut être en mesure de voir ce qui se trouve sur votre écran, y compris les documents sensibles, alors pensez à vous procurer un filtre de confidentialité pour écran. N'oubliez pas non plus que n'importe qui peut écouter vos appels téléphoniques professionnels et utiliser les informations sensibles que vous partagez. Il est toujours préférable de discuter de sujets confidentiels uniquement lorsque vous êtes sûr de ne pas être écouté.

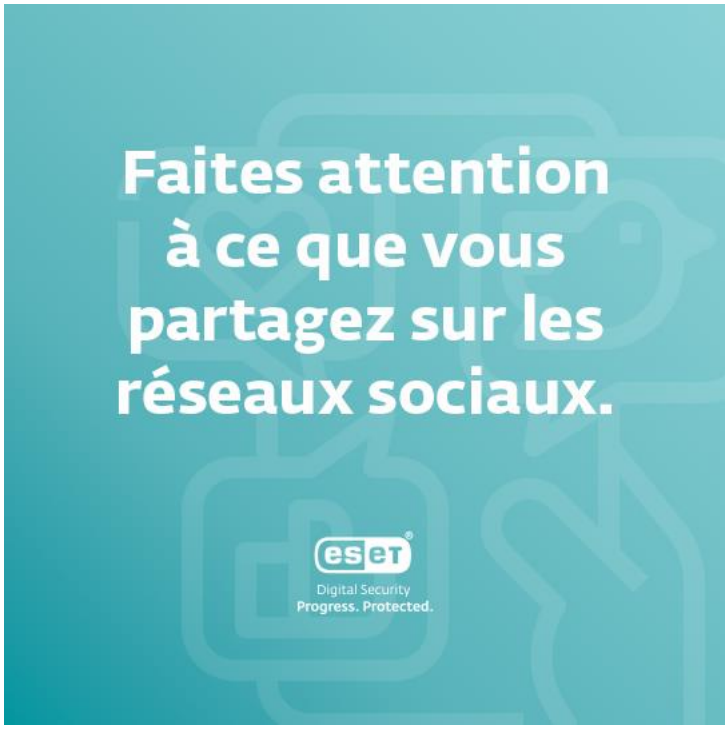


Prenez 30 minutes pour configurer votre routeur Wifi personnel. Cela vaut le coup...

Le télétravail est devenu une norme pour beaucoup d'entre nous. Remplacez vos identifiants par défaut (notamment le nom et le mot de passe par défaut de votre accès Wifi) par un mot de passe sûr ou une phrase de passe. Vous devez également désactiver la gestion à distance, maintenir votre micrologiciel à jour et activer le chiffrement du réseau, idéalement WPA3. Vous ne savez pas comment faire ? Voici quelques conseils, et si vous n'êtes toujours pas sûr de la marche à suivre, vous pouvez toujours contacter votre service informatique. Sans ces mesures préventives, il est assez facile pour tout intrus extérieur d'accéder à vos données, tant professionnelles que personnelles.

Découvrez si vos identifiants de connexion ont été compromis.

Rendez-vous sur le site web Have I Been Pwned, saisissez votre adresse email et découvrez si vos identifiants ont fait l'objet d'une fuite de données. Si c'est le cas, mettez en place un mot de passe renforcé sur les comptes compromis, et tous les autres.



Faites attention à ce que vous partagez sur les réseaux sociaux.

Vous voulez partager un selfie depuis le bureau ? Ou une photo amusante de votre espace de travail ? En montrant à d'autres l'environnement dans lequel vous travaillez, un intrus pourrait facilement s'orienter et donner l'impression d'y être à sa place. Vous pourriez également partager sans le savoir certaines informations sensibles sur vos collègues, votre employeur ou vous-même, par exemple, si la photo de votre bureau montre des documents sensibles ou des post-it avec des identifiants. Avant de partager quoi que ce soit en rapport avec votre activité professionnelle, assurez-vous que cela n'impacte pas la sécurité des données des collaborateurs, de l'entreprise ou de vous-même.

Partager, c'est aimer, comme on dit, mais pas lorsqu'il s'agit d'appareils professionnels.
Même s'il est tentant de laisser vos enfants utiliser votre ordinateur professionnel pour jouer ou regarder un film, votre appareil contient des données qui ne doivent être partagées avec personne à l'extérieur de votre lieu de travail. Il suffit de quelques clics imprudents pour que les données sensibles de votre ordinateur portable soient exposées de façon parfois irrémédiable. Idéalement, n'utilisez les appareils professionnels que pour des pratiques liées au travail et ne laissez personne d'autre y avoir accès.

Sachez quoi faire lorsque vous égarez votre appareil professionnel.

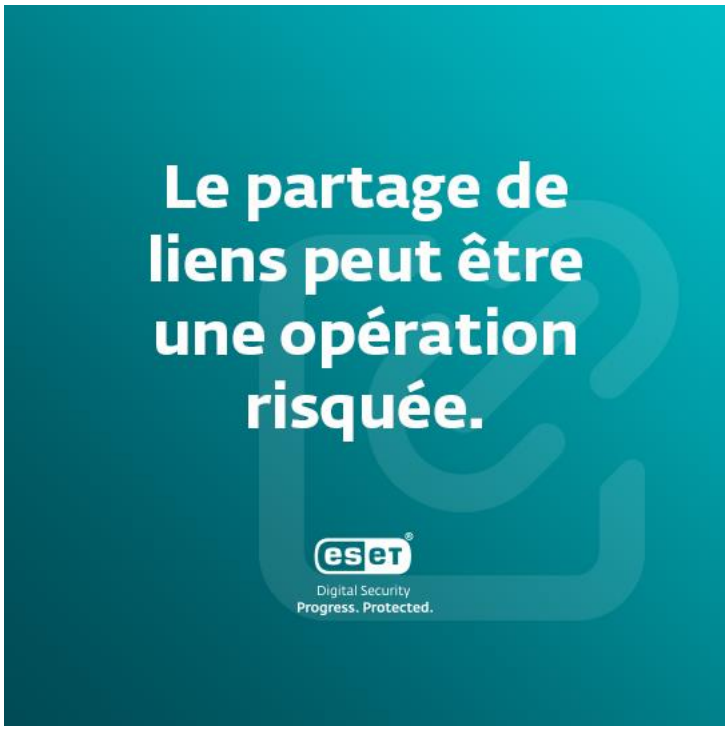
La perte de votre appareil professionnel est désagréable, mais nous savons tous que cela peut arriver. En plus d'être prudent avec les équipements de votre entreprise (vous en êtes responsable), vous devez savoir quoi faire lorsqu'une telle situation se produit. N'hésitez pas à contacter votre service informatique afin qu'il puisse résoudre le problème rapidement. Et même si vous n'avez jamais perdu d'appareil professionnel, il vaut mieux y être préparé. Demandez à votre service informatique ce qu'il faut faire dans ces situations et familiarisez-vous avec la procédure appropriée.

Ne retardez pas les mises à jour.

Si une fenêtre pop-up vous demandant de mettre à jour vos applications ou vos logiciels vous surprend, n'hésitez pas à contacter le service informatique. L'utilisation d'une version obsolète d'une application ou d'un logiciel peut vous faire courir un risque inutile. Les responsables IT doivent par ailleurs vérifier si les nouvelles versions sont aussi sûres que les anciennes.

N’utilisez que les canaux désignés pour les communications liées au travail.

Qu’il s’agisse de partager un document sensible ou demander à un collègue de déjeuner avec vous, il existe des canaux appropriés à utiliser et qui ont été choisis en fonction de leur niveau de sécurité et adaptés à chaque situation. En utilisant des applications non approuvées, vous risquez de rendre vos messages et vos documents accessibles à des personnes extérieures à votre société, la mettant ainsi en danger par une éventuelle fuite de données. Assurez-vous de connaître les sites et les applications que vous pouvez utiliser pour communiquer, et si vous n’êtes pas sûr, n’hésitez pas à en discuter avec vos spécialistes informatiques.



Le partage de liens peut être une opération risquée.

Vous devez communiquer un document sensible à un collègue ? Plutôt que de créer un lien de partage public, autorisez l'accès directement aux personnes que vous avez choisies et qui ont vérifié leur identité. Idéalement, optez pour un accès limité dans le temps si vous partagez des fichiers avec des personnes externes à l'entreprise. De même, le partage de documents professionnels sur des adresses email privées est à proscrire. Pourquoi ? Afin de minimiser le risque de transmettre des informations aux mauvais destinataires.

N’hésitez pas à consulter votre spécialiste informatique.

Vous hésitez sur la bonne posture à adopter lorsque vous recevez un email suspect ? Vous ne savez pas comment partager un document en toute sécurité avec vos collègues ? Aucune question n’est inutile, alors n’ayez pas peur d’interroger votre département informatique. Ne craignez pas de leur faire perdre leur temps : votre responsabilité et les précautions que vous prenez pourraient leur épargner beaucoup de temps et d’ennuis à long terme. Il est toujours préférable de rester informé et protégé plutôt que d’affronter des problèmes plus graves et d’en subir les conséquences ultérieurement. La prévention et la communication sont la clé d’une bonne cyberhygiène en entreprise et chez vous !