GUIDE DE WIREDSCORE...

POUR PROTÉGER VOTRE RÉSEAU

CONTRE LES CYBERATTAQUES

GUIDE DE WIREDSCORE...

POUR PROTÉGER VOTRE RÉSEAU

CONTRE LES CYBERATTAQUES

Il n'y a pas d'honneur parmi les voleurs. Tel est le cas, même en pleine crise sanitaire internationale.

Alors que tout le monde se tourne vers le télétravail, l'éducation à distance et les distanciations sociales pour endiguer la propagation du Covid-19, les cybercriminels ont saisi l'opportunité de tirer parti de notre dépendance collective à la connectivité.

Bien que les entreprises et établissements scolaires puissent limiter les risques d'attaques sur leurs réseaux quand les utilisateurs sont dans leurs locaux, l'accès à distance rend nos réseaux beaucoup plus vulnérables..

Suivez les conseils simples de ce guide et protégez votre vie privée.

Dans ce petit guide, nous expliquerons les types d'attaques les plus souvent subies par les télétravailleurs.

Mais ne vous inquiétez pas. Vous pouvez mettre en place de simples actions pour vous protéger contre les cybercriminels opportunistes.

Dans la seconde partie de ce guide, nous vous montrerons ce que vous devez faire pour rester protégés.

LES CYBERATTAQUES LES PLUS COURANTES PENDANT LE COVID-19

Au cours des dernières semaines, nous avons observé une hausse des cybercrimes ; du piratage psychologique à l'hameçonnage en passant par les attaques par force brute sur nos réseaux domestiques.

Les hackers n'ont aucune honte et auront recours à tous les moyens pour obtenir vos données. Cette tendance ne fait qu'augmenter quand nous sommes distraits par des évènements d'ampleur mondiale, même l'Organisation mondiale de la santé a été attaquée en mars dernier.

90 % des cyberattaques commencent avec une campagne d'hameçonnage et les hackers adaptent leurs méthodes afin de profiter du nombre croissant de télétravailleurs.

90 % des cyberattaques commencent avec une campagne d'hameçonnage, et les hackers adaptent leurs méthodes afin de profiter du nombre croissant de télétravailleurs.

Voici les méthodes les plus courantes d'hameçonnage utilisées pour voler vos informations personnelles :

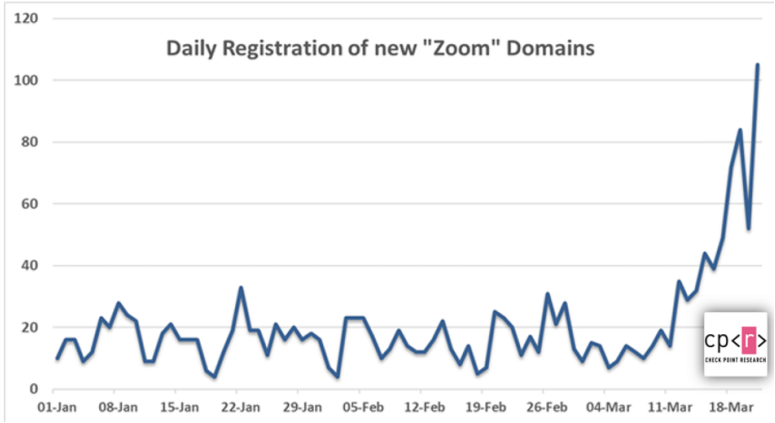
Sites d'hameçonnage

Ces sites internet sont créés pour amener les utilisateurs à les visiter lorsqu'ils font une faute de frappe en tapant le nom d'un site ou en cliquant sur un lien qui ressemble à celui du vrai site.

Un site d'hameçonnage essaye de voler vos mots de passe ou autres informations confidentielles en vous faisant croire que c'est un véritable site sécurisé.

Pendant une crise comme le Covid-19, les hackers augmentent le nombre d'attaques en enregistrant autant de domaines que possible avec les mots-clés les plus recherchés.

- Selon l'entreprise de logiciel, **Checkpoint,** Selon l'entreprise de logiciel, Checkpoint, depuis le début de 2020, il y a eu une augmentation considérable des nouveaux noms de domaines enregistrés qui incluent « Zoom », le nom du logiciel de visioconférence. Depuis janvier, il y a eu 1700 nouveaux domaines enregistrés avec une variation de « Zoom », dont 25 % ont été enregistrés durant la seconde semaine d'avril uniquement.
- Google a aussi connu une augmentation de 350 % des sites d'hameçonnage voulant profiter de notre désir d'information en se faisant passer pour des organisations de santé, des associations caritatives et des instituts de recherche. En janvier 2020, 149 195 sites d'hameçonnage associés au Covid-19 au total sont devenus actifs. Ce nombre a fait un bond de 100%, passant à 293 235 en février, et a presque doublé encore en mars, pour un total de 522 495 sites d'hameçonnage enregistrés liés au Covid-29.



Emails d’hameçonnage

Si vous voulez voir à quoi ils ressemblent, regardez vos courriels indésirables ! Nous avons tous vu ces emails : ils sont généralement mal écrits, souvent envoyés par quelqu’un que nous connaissons et tentent de nous faire télécharger une pièce jointe pour lancer un logiciel malveillant sur notre ordinateur.

Quel est le problème alors si ma boîte de courriels indésirables les capturent tous ?

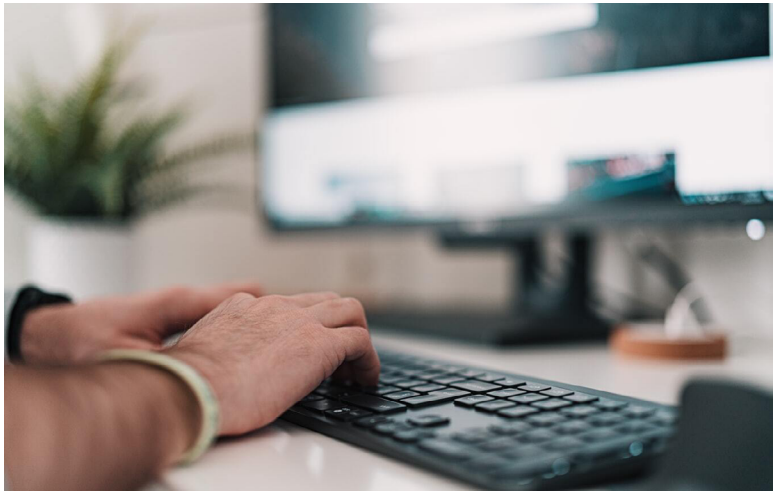
Malheureusement, beaucoup contournent votre boîte de courriels indésirables et arrivent dans votre boîte de réception. Les cybercriminels deviennent de plus en plus intelligents et les fournisseur de messagerie électronique doivent continuellement rattraper leur retard.

Il existe plusieurs types d'email d'hameçonnage auxquels vous devez faire attention :

Informations d'entreprise : Les cybercriminels ciblent les employés en télétravail avec des messages de l'entreprise leur notifiant qu'un cas positif au Covid-19 a été signalé au sein de l'entreprise. Le message contient des pièces jointes malveillantes déguisées en protocoles mis en place par l'entreprise ainsi qu'une « brochure » que les destinataires doivent ouvrir, lire et imprimer.

Informations gouvernementales et liées au Covid-19 : Il y a eu de nombreuses tentatives d'envoi d'emails de la part d'organisations officielles en apparence, qui demandent des contributions charitables ou proposent une aide financière, un remboursement de la part d'une compagnie aérienne, de faux traitements et vaccins ainsi que de faux kits de test.

Aux Etats-Unis, les américains vont recevoir des « stimulus checks » au second semestre, mais le FBI avertit que les hackers en profiteront pour voler des informations via des emails d'hameçonnage. Ils ont prévenu qu'en aucun cas les agences gouvernementales ne contacterons les citoyens pour leur demander des informations personnelles.



COMMENT SE PROTÉGER CONTRE LES SITES ET EMAILS D'HAMEÇONNAGE ?

- Vérifiez le contenu de l'email, cherchez des mots mal écrits et examinez attentivement l'adresse email de retour. Normalement, ces emails sont particulièrement vagues ou généraux.

- N'ouvrez pas les pièces jointes inconnues et ne cliquez pas sur les liens présents dans les emails ou les SMS.

- Faites attention aux faux noms de domaines et vérifiez que vous êtes sur un site sécurisé avec la bonne URL avant d'entrer votre mot de passe ou informations personnelles.

- Examiner le domaine de l'adresse email de l'expéditeur pour en vérifier la légitimité.

- Exemple : expediteur@wiredscore.com WiredScore.com est un vrai site.

Maintenant vous savez comment vous protéger contre les cyberattaques que vous pouvez typiquement rencontrer et identifier, mais qu'en est-il des autres attaques ?

SÉCURITÉ DU RÉSEAU DOMESTIQUE

Malheureusement, il n'y a pas qu'un seul instrument dans la boîte à outil de l'hacker et les hackers les plus sophistiqués vont cibler les réseaux auxquels nous nous connectons plutôt que d'utiliser des sites ou des emails. Les réseaux domestiques, par nature, ne sont pas aussi sécurisés que les réseaux d'entreprise et les hackers cherchent à exploiter cette vulnérabilité.

Voici quelques actions simples que vous pouvez mettre en place pour améliorer la sécurité de votre réseau domestique :

Comment sécuriser votre routeur et votre Wi-Fi

Depuis début mars, il y a eu une augmentation des attaques sur les routeurs domestiques.

Les attaquants utilisent la « force brute » pour infiltrer nos réseaux ; cela signifie qu'ils utilisent des logiciels qui essayent des milliers de combinaisons de mots de passe jusqu'à ce qu'ils s'infiltrent.

Une fois infiltrés, les hackers changent les paramètres de nos routeurs pour nous diriger automatiquement vers les sites d'hameçonnage comme ceux mentionnés ci-dessus.

Les attaquants utilisent la « force brute » pour infiltrer nos réseaux ; cela signifie qu'ils utilisent des logiciels qui essayent des milliers de combinaisons de mots de passe jusqu'à ce qu'ils s'infiltrent.

QUATRE ÉTAPES FACILES POUR SÉCURISER VOTRE RÉSEAU DOMESTIQUE

1. **Changer le mot de passe par défaut de votre routeur et Wi-Fi :**

Si vous êtes comme la plupart d'entre nous, vous utilisez un routeur fourni par votre Fournisseur d'Accès Internet (FAI) et vous n'avez pas changé le mot de passe ou les informations du Wi-Fi par défaut, ce qui représente une grosse faille de sécurité. La majorité de ces mots de passe sont facilement piratables. Il y a même un site qui recense **les mots de passe par défaut des routeurs** pour aider ceux qui n'arrivent pas à y accéder - c'est un cadeau pour les cybercriminels.

La plupart des routeurs sont accessibles via une page web, mais consultez le site de votre FAI pour trouver les instructions d'accès à votre routeur qui devraient ressembler à ceci :

- Quand vous ouvrez votre navigateur, vous devrez vous rendre sur une page web dont l'URL est une série de chiffres, souvent imprimée au dos de votre routeur et ressemble à quelque chose comme **https://192.168.1.1**
- Connectez-vous au routeur avec **le mot de passe de l'administrateur (sur le dos de votre routeur).**
- Le nom d'utilisateur est **"admin"**. Vous pouvez trouver le mot de passe de l'administrateur par défaut sur l'étiquette de votre routeur.
- Remplacez le mot de passe actuel de l'administrateur par un nouveau mot de passe fort et facile à mémoriser pour vous. Suivez les instructions détaillées à l'écran ou dans le guide utilisateur de votre routeur.
- Maintenant faites de même pour le mot de passe de votre Wi-Fi (choisissez-en un différent de celui du routeur). Remplacez-le par un mot de passe fort en choisissant une longue suite de chiffres, lettres et symboles. Votre mot de passe doit être de 12 caractères minimum (n'oubliez pas de reconnecter tous les appareils connectés au Wi-Fi).

- Procédez ensuite aux étapes 2 et 3 tout en restant sur la page web des paramètres de votre routeur.

2. Gardez le micrologiciel de votre routeur à jour

Une fois connecté à votre routeur (voir étape 1), assurez-vous qu'il n'y a pas de mises à jour en attente. La plupart des routeurs les téléchargent automatiquement, mais beaucoup d'anciens appareils requièrent une mise à jour manuelle. Assurez-vous de télécharger la dernière version du logiciel.

3. Désactivez le WPS (Wi-Fi Protected Setup)

Le WPS vous permet de connecter de façon rapide et simple votre routeur Wi-Fi à vos appareils (un smartphone, par exemple), soit par un bouton sur le routeur, soit par un code PIN imprimé sur un sticker. Il y a quelques années, une vulnérabilité grave a été identifiée dans de nombreuses implémentations de WPS par des FAI. Cette vulnérabilité permet aux hackers de s'introduire dans les réseaux et donne également à toute personne ayant un accès physique à votre routeur la possibilité de s'y connecter.

Puisqu'il est difficile de déterminer quel modèle de routeur et quelle version du micrologiciel sont vulnérables, il est préférable de simplement désactiver cette fonctionnalité, ce qui peut être fait en vous connectant à votre routeur. Vous devriez avoir toutes les instructions nécessaires pour le faire en cherchant sur Google « désactiver WPS <nom du Fournisseur d'Accès Internet> ».

4. Activer le meilleur niveau de sécurité

Dans « paramètres de sécurité » ou une section similaire dans votre routeur, assurez-vous que la sécurité de votre réseau est sur le mode WPA2-PSK [AES] ou le réglage le plus élevé disponible. WPA2-PSK [AES] est actuellement le niveau le plus élevé disponible pour les réseaux domestiques sans fil.

COMMENT SÉCURISER VOS APPAREILS

1. Gardez vos appareils connectés à jour

C'est bien d'avoir un routeur sécurisé, mais ce sera inutile si vous repoussez vos mises à jour Windows ou iOS depuis 2 ans. Chaque appareil connecté à votre réseau pourrait constituer un accès caché à tous vos appareils. Installez les correctifs de sécurité et les mises à jour comme recommandé par les systèmes d'exploitation de votre ordinateur (Windows ou macOS) et de vos appareils mobiles, étant donné que tous les fabricants corrigent continuellement les nouvelles failles de sécurité. Si vous ne savez pas comment faire, recherchez sur Google « comment mettre à jour le logiciel <Windows ou mac> ».

2. Activer le pare-feu sur votre ordinateur

Un pare-feu est une fonctionnalité de sécurité destinée à vous aider à protéger votre ordinateur et vos données personnelles contre un accès non-autorisé et à vous alerter en cas de risques imminents. La plupart des appareils ont un pare-feu intégré et il suffit de l'activer. Voici comment faire en fonction de votre appareil :

a. **Sur Mac**, choisissez Menu Apple > Préférences Système, cliquez sur Sécurité et confidentialité, puis sur Coupe-feu. … Cliquez sur Options de Coupe-feu. Si les options de coupe-feu sont désactivées, cliquez d'abord sur Activer le coupe-feu.

b. **Sur Windows**, entrer Pare-feu dans votre barre de recherche Cortana. Cliquez sur Pare-feu Windows dans les résultats de recherche. Dans la fenêtre qui s'affiche, assurez-vous que le Pare-feu Windows est activé. S'il ne l'est pas, cliquez sur Activer le Pare-feu Windows dans la partie gauche de la fenêtre.

3. « Maison intelligente » et streaming sécurisé

La plupart des appareils IoT (Internet of Things) et des appareils de streaming (Roku, Fire TV Stick, Apple TV) ont aussi un mot de passe par défaut qu'il suffit de rechercher sur Google. Nous recommandons fortement de changer les mots de passe sur ces appareils en utilisant le manuel utilisateur, et de vérifier également que les mises à jour du logiciel se font automatiquement. Une bonne pratique est aussi de connecter ces appareils à un réseau « invité » séparé de votre routeur afin de les séparer de vos téléphones et ordinateurs, qui contiennent plus de données personnelles.

Le label WiredScore est un système d'évaluation internationalement reconnu pour les immeubles de bureaux permettant aux propriétaires de concevoir et de promouvoir la connectivité de leurs immeubles auprès des utilisateurs.

Les employés travaillant dans des bâtiments labellisés WiredScore ont l'avantage de savoir que leurs entreprises sont soutenues par les technologies les plus récentes en matière de connectivité.

Si vous êtes propriétaire ou locataire et que vous souhaitez savoir comment labelliser votre bâtiment, prenez rendez-vous avec notre équipe en cliquant sur le bouton ci-dessous.

CONTACTEZ-NOUS

Précision sur le contenu : Cet article s'adresse aux utilisateurs à la maison et aux clients ayant des besoins basiques en internet. Beaucoup de nos clients utilisent des VPN pour se connecter à des réseaux d'entreprise, ce qui représente actuellement le plus gros risque. Cela pourrait faire l'objet d'un autre article concernant les considérations à prendre en compte afin d'accéder à votre réseau d'entreprise en toute sécurité.

Auteur : John Meko, Directeur de l'Ingénierie, Amérique du Nord, WiredScore

- How to protect yourself from cyberattacks when working from home during COVID-19
- Governments experience surge in cyberattacks
- Zoom Domains Targeted by Hackers, as Use Surges with COVID-19
- COVID-19 Cyber Threats: Hackers Target DNS Routers, Remote Work
- COVID-19 Phishing Schemes Escalate; FBI Issues Warning