Le manuel du télétravail pour les experts en cybersécurité

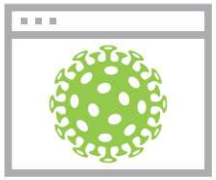
CARBONITE
an opentext company

WEBROOT
an opentext company

La technologie n'a de cesse d'évoluer, de même que les cyberattaques.

Chaque jour, les pirates imaginent de nouvelles façons de pénétrer les systèmes, de dérober des données et de causer des problèmes. En plus de cela, ils profitent des événements actuels (comme la COVID-19) en jouant sur la peur, la confiance et le désir de tout un chacun de s'informer d'une manière générale.

Webroot a identifié au moins 20 000 nouveaux sites Web créés en mars et avril 2020 suite à la pandémie de COVID-19, ou coronavirus.



Selon nos données stratégiques sur les menaces, au moins 2 % de ces sites Web sont malveillants. En plus de cela, nous avons observé une hausse significative des campagnes de phishing ciblées prétendant offrir des informations liées à la COVID-19, des équipements de protection individuelle (EPI) telles que les masques, des conseils de santé du gouvernement, etc.

De plus en plus d'individus travaillent, étudient et interagissent en ligne, par conséquent il est essentiel que nous prenions des mesures de cybersécurité adéquates pour nous protéger, nous et nos familles, contre les menaces et les cyberattaques en constante évolution.

C'est pourquoi nous avons élaboré ce manuel sur le télétravail, qui rassemble des conseils simples à appliquer pour vous aider à mettre en place votre propre installation technologique conviviale et bien informée à domicile. Ce manuel s'articule en trois parties et vous apprendra ce que vous devez savoir au sujet des cyberattaques et expliquera comment identifier les failles de sécurité et y remédier, afin que vous et votre famille soyez protégés contre les pirates et leurs tactiques.

[1] Sur la base des observations de Webroot sur les menaces et l'analyse interne, réalisée en avril 2020

PARTIE UN

Comprendre contre quoi vous luttez

La première étape pour assurer une stratégie de télétravail efficace et sécurisée consiste à déterminer contre quoi vous luttez. Dans cette section, nous aborderons certains types de cyberattaques courantes que vous pourriez rencontrer avec votre informatique à la maison. Bien que cette liste ne soit pas exhaustive, elle vous aidera à mieux comprendre les types d'attaques de base que les pirates malveillants peuvent employer.

Vue d'ensemble des attaques courantes

Phishing

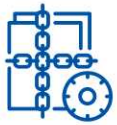
De quoi s'agit-il ?
Une attaque conçue pour obtenir frauduleusement des informations sensibles telles que les noms d'utilisateur, les mots de passe et les numéros de carte bancaire, etc.

En quoi cela consiste-t-il ?
Les criminels se font passer pour une entité digne de confiance, comme une banque, un prestataire de soins de santé ou même votre supérieur hiérarchique, via un e-mail, un message SMS, un message sur les réseaux sociaux ou toute autre communication électronique, pour vous inciter à remettre des informations sensibles, privées ou d'autres informations personnelles. Grâce à ces informations, les criminels peuvent accéder à vos comptes en ligne, commettre des fraudes, usurper et vendre votre identité, etc.

Logiciels malveillants

De quoi s'agit-il ?
Un logiciel malveillant est un terme générique qui fait référence aux chevaux de Troie, aux virus, aux vers, aux rançongiciels et à d'autres cybermenaces qui peuvent être installées sur l'appareil d'une victime.

En quoi cela consiste-t-il ?
Les logiciels malveillants sont conçus pour infiltrer ou endommager votre système informatique ou votre appareil mobile sans votre consentement éclairé. Différents types de logiciels malveillants font des choses différentes, mais peuvent crypter ou verrouiller l'accès à vos fichiers (voir Rançongiciels), dérober vos données personnelles (voir enregistreurs de frappe et suivi système), et bien plus encore.



Rançongiciels

De quoi s'agit-il ?
Un type de logiciel malveillant qui bloque l'accès aux données des victimes en chiffrant leurs fichiers ou l'intégralité de leur disque dur.

En quoi cela consiste-t-il ?
Le rançongiciel bloque l'accès à vos fichiers ou disques durs, puis vous demande de payer une rançon, généralement en crypto-monnaie, pour récupérer vos fichiers. Cela peut être l'un des types de logiciels malveillants les plus dévastateurs que vous puissiez rencontrer, car il est impossible de décrypter des fichiers verrouillés sans la clé de cryptage unique utilisée par les pirates. Cela signifie qu'à moins d'avoir une sauvegarde sécurisée en place, il n'y a aucun moyen de récupérer vos fichiers sans payer la rançon.

Logiciels espions (Spywares)

De quoi s'agit-il ?
Un type de logiciel malveillant qui fonctionne pour recueillir des informations sur une personne ou une organisation à son insu.

En quoi cela consiste-t-il ?
Les logiciels espions collectent silencieusement des informations en arrière-plan, puis les envoient à une autre entité sans votre consentement ou avec le consentement via les cookies. Il peut également prendre le contrôle d'un appareil à votre insu, ce qui permet aux acteurs malveillants d'utiliser des parties de votre système comme bon leur semble.

Enregistreurs de frappe et suivi système

De quoi s'agit-il ?
Logiciel qui enregistre ouvertement ou secrètement les actions des utilisateurs et / ou les processus système et fournit ces enregistrements pour examen, soit par l'utilisateur, soit par un tiers.

En quoi cela consiste-t-il ?
Les enregistreurs de frappe et les suivis système enregistrent les frappes au clavier et autres actions sur votre système, y compris les activités de connexion et les informations d'identification, les mots de passe et le contenu des e-mails, les données de comptes financiers et de transactions, les numéros de carte bancaire, les numéros de sécurité sociale, etc. C'est l'une des méthodes les plus couramment utilisées par les cybercriminels pour accéder à vos comptes et commettre une usurpation d'identité ou une fraude.

Virus

De quoi s'agit-il ?
Le plus ancien type de logiciel malveillant, un virus attache son code à d'autres programmes pour se multiplier en altérant le programme et ses applications.

En quoi cela consiste-t-il ?
Les virus modifient le programme infecté et ses applications en attachant du code viral et en se multipliant. Vous pouvez contracter un virus en partageant des données, des fichiers et de la musique avec d'autres personnes, en visitant un site Web infecté, en ouvrant un e-mail de spam ou une pièce jointe malveillante, ou en téléchargeant des applications, des barres d'outils et des jeux gratuits à partir de sources non vérifiées. Au mieux, ces virus nuiront aux performances de votre ordinateur. Au pire, ils peuvent endommager les programmes, supprimer des fichiers importants et même neutraliser votre ordinateur.

Vers

De quoi s'agit-il ?
Un type de logiciel malveillant conçu pour se propager en se dupliquant rapidement d'un système à l'autre.

En quoi cela consiste-t-il ?
Les vers se propagent autant que possible pour exécuter les commandes des attaquants, telles que la suppression de fichiers et la livraison d'autres charges utiles de logiciels malveillants (par exemple, un rançongiciel). Si vous avez plusieurs appareils connectés ou mis en réseau ensemble, un ver peut continuer à se propager à partir du premier appareil jusqu'à infecter tous vos appareils connectés.

Chevaux de Troie

De quoi s'agit-il ?
Les chevaux de Troie sont un type de logiciel malveillant qui est généralement installé sans le consentement complet ou éclairé d'un utilisateur, et se composent généralement d'un compte-gouttes, d'une porte dérobée, d'un robot, d'un phisher et d'un relais ; ils peuvent être contrôlés à distance.

En quoi cela consiste-t-il ?
Les chevaux de Troie s'installent sans votre consentement et activent le contrôle à distance depuis un autre appareil. Ils procèdent ensuite au transfert des informations sensibles, reçoivent des instructions de la part des attaquants, compromettent davantage votre appareil, etc.

DEUXIÈME PARTIE

Configurer un espace de télétravail productif

La deuxième étape pour garantir une stratégie de télétravail efficace et sécurisée consiste à configurer correctement votre espace de travail physique. Avec quelques conseils, astuces et éléments de maintenance simples d'application, vous pouvez booster votre productivité et votre confort lorsque vous travaillez ou étudiez à la maison.

Assurez-vous que votre environnement est confortable et (surtout) sans distraction.

Assurez-vous de disposer d'un espace de travail désigné avec une chaise confortable (regardez les chaises prévues pour jouer aux jeux vidéos, par exemple), de préférence dans une pièce privée. Vous pouvez également envisager un bureau sur pied, pour ne pas être obligé de rester assis toute la journée. Certains bureaux sont réglables, vous pouvez donc les utiliser debout ou assis. Faites régulièrement des pauses durant lesquelles vous vous éloignez de l'ordinateur ; par exemple, faites une promenade ou asseyez-vous dehors pendant un moment. Cela vous aidera à rester plus concentré sur le long terme.

Désencombrez votre espace souvent.

L'encombrement est une distraction qui peut vous donner le sentiment d'être dépassé. Nous ne parlons pas seulement des bibelots physiques qui se trouvent un peu partout dans votre maison. Pensez également à tous les fichiers inutiles ou mal organisés sur votre ordinateur, qui représentent un fouillis numérique. Veillez à maintenir votre espace de travail et vos appareils professionnels exempts de ces distractions stressantes.

Délimitez une frontière claire entre vos vies personnelle et professionnelle.

Lorsque vous êtes en train de travailler, les tâches personnelles sont une distraction. Mais penser au travail durant le dîner vous déconnectera de votre famille et de vos amis. Déterminez un planning cohérent qui vous convient, même s'il ne s'agit pas du « 9 h - 17 h » typique, afin de pouvoir séparer vos vies personnelle et professionnelle tout en accomplissant vos tâches comme un professionnel.

Délimitez une frontière claire entre vos appareils personnels et professionnels.

Vous ne pouvez peut-être pas toujours vous accorder le luxe de disposer d'appareils distincts et dédiés pour vos activités personnelles et professionnelles. Mais si vous avez plusieurs appareils, assurez-vous d'utiliser les appareils professionnels pour le travail et les appareils personnels pour vos occupations personnelles. C'est plus sûr, à la fois pour l'entreprise et pour vous.

PARTIE TROIS

Renforcez votre cyber-environnement

Lorsque nous ne bénéficions pas de la présence d'un personnel d'assistance informatique dédié, il est important de prendre en main sa cybersécurité. La troisième et dernière étape pour assurer une stratégie efficace et sécurisée en termes de télétravail consiste à identifier et à combler toutes les failles de sécurité.

Assurez-vous que TOUS vos appareils sont sécurisés.

Que vous utilisiez un ordinateur portable, un ordinateur de bureau, une tablette, un téléphone, un appareil Windows®, MacOS®, iOS® ou Android®, vous devriez utiliser un logiciel de cybersécurité et une sauvegarde.

Antivirus

La chose la plus élémentaire dont vous avez besoin sur tous vos appareils est un produit antivirus. ***Gardez à l'esprit qu'il existe de nombreuses options « gratuites » qui n'incluent pas toutes les fonctionnalités, ne prévoient aucun support technique ou contiennent des logiciels publicitaires qui diffusent d'innombrables publicités potentiellement malveillantes (et tout simplement ennuyeuses) sur votre appareil.*** Utilisez un produit réputé, de préférence avec un abonnement payant, pour ne pas avoir à vous soucier des publicités et obtenir facilement de l'aide si vous en avez besoin.

VPN

Même lorsque vous avez installé un antivirus, votre connexion à Internet reste vulnérable. Pensez à la navigation sur le Web comme s'il s'agissait d'un voyage en voiture. Si vous conduisez sur une route dégagée, tout le monde peut voir où vous êtes allé, comment vous y êtes arrivé, où vous vous êtes arrêté, etc. Mais si vous avez parcouru tout le chemin à travers votre propre système de tunnels PRIVÉS, que personne d'autre ne peut utiliser, alors personne ne pourra vous espionner. Un VPN vous offre ce tunnel privé, ainsi vous savez que vous et vos données resterez en sécurité.

Sauvegarde

Si vous perdez tout à coup l'accès à tous vos fichiers, personnels ou professionnels, les retombées peuvent être dévastatrices. De plus, dans le cas de fichiers professionnels, il est plus difficile pour le personnel informatique de résoudre ces problèmes si vous travaillez à distance. ***Assurez-vous d'effectuer une sauvegarde régulière pour un stockage cloud sécurisé et crypté***.

Soyez à jour en termes de mises à jour logicielles.

Certaines des parties de votre appareil les plus faciles à exploiter pour les cybercriminels font partie de programmes totalement légitimes, mais obsolètes. Veillez à maintenir tous vos systèmes d'exploitation et applications logicielles à jour et à exécuter tous les correctifs disponibles, pour combler ces failles de sécurité.

Activez l'authentification à deux facteurs et utilisez des mots de passe robustes et uniques.

Si vous réutilisez les mêmes mots de passe sur différentes connexions, vous facilitez la tâche aux cybercriminels qui tentent d'usurper votre identité et de dérober vos données, car ils n'ont alors qu'à s'emparer d'un seul mot de passe pour accéder à plusieurs comptes. ***Utilisez toujours des mots de passe robustes et uniques et activez l'authentification à 2 facteurs dans la mesure du possible***. Vous pouvez utiliser un gestionnaire de mots de passe pour vous aider à créer et à stocker des mots de passe robustes. De cette façon, vous n'avez pas à vous souvenir de tous ou à les écrire.

Gardez vos données pour vous.

Limitez les informations que vous partagez en ligne, la manière dont vous les partagez et avec qui. En étant extrêmement prudent quant à la quantité de données personnelles que vous partagez et à quel moment, vous devenez une cible moins attrayante pour les cybercriminels.

Restez vigilant.

- Les cybercriminels sont toujours à la recherche de nouvelles possibilités ***pour vous escroquer, en exploitant la peur ou les actualités du moment,*** afin d'attirer votre attention.
- Traitez chaque e-mail ou message comme s'il ***pourrait s'agir d'une arnaque de phishing***.
- ***Faites preuve d'une extrême prudence*** lorsque vous cliquez sur des liens et en téléchargeant des fichiers, même de la part d'individus que vous connaissez.
- Si vous recherchez des informations qu'un e-mail prétend offrir, ***ne cliquez sur aucun lien***. Utilisez un moteur de recherche tel que Google ou Bing pour trouver un site Web officiel (par exemple, si vous souhaitez obtenir des détails sur la COVID-19, allez directement sur le site officiel des autorités gouvernementales.)
- ***Si vous téléchargez un fichier et qu'il vous demande d'activer des macros, NE LE FAITES PAS. Il s'agit d'une tactique cybercriminelle courante pour installer des logiciels malveillants sur votre système***. Il existe très peu de raisons légitimes pour qu'un document utilise des macros, et ces raisons ne s'appliquent généralement pas à la situation lambda d'un utilisateur à domicile.

Pour beaucoup, travailler ou étudier à domicile est la « nouvelle norme ».

Il est important que nous trouvions tous des moyens de rester en bonne santé, productifs et en sécurité, peu importe où nous sommes ou ce que la vie nous réserve. En suivant les étapes de ce manuel, vous êtes sur la bonne voie pour atteindre ces objectifs, aujourd'hui et à l'avenir.

Que vous soyez un novice en cybersécurité ou un gourou de l'informatique chevronné, Webroot est là pour vous protéger et vous guider à travers les hauts et les bas d'un cyber-paysage en constante évolution. C'est pourquoi nous vous proposons des conseils, des astuces et des bonnes pratiques pour tous vos besoins Internet, du télétravail à la rentrée scolaire, en passant par les achats de vacances sécurisés et la configuration de nouveaux appareils, afin que vous soyez protégé contre les pirates et les cybermenaces.

En savoir plus. Si vous avez des questions au sujet de l'amélioration de vos habitudes de cybersécurité, n'hésitez pas à nous contacter au +33 14 777 0500.

CARBONITE
an opentext company

WEBROOT
an opentext company

carbonite.fr | webroot.com/fr/fr

À propos de Webroot et de Carbonite

Les sociétés Carbonite, Webroot et OpenText exploitent le Cloud et l'intelligence artificielle pour fournir des solutions complètes de cyber-résilience aux entreprises, aux particuliers et aux fournisseurs de services gérés. La cyber-résilience signifie pouvoir rester opérationnel, même face aux cyberattaques et à la perte de données. C'est pourquoi nous avons uni nos forces pour fournir des solutions de protection des points de terminaisons et des réseaux, de sensibilisation à la sécurité et de sauvegarde des données et de reprise après sinistre, ainsi que des services de renseignement sur les menaces utilisés par les principaux fournisseurs de technologies du marché dans le monde entier. Nous exploitons la puissance de l'apprentissage automatique pour protéger des millions d'entreprises et de particuliers, et sécuriser le monde connecté. Webroot et Carbonite sont implantés en Amérique du Nord, en Europe, en Australie et en Asie. Découvrez la cyber résilience sur carbonite.com et webroot.com.