Tout sur la sécurité préventive

Sommaire :

Pirates sur Snapchat / Cyberharcèlement / Protégez-vous des courriers indésirables / En savoir plus sur le phishing / La différence entre un logiciel antivirus et un logiciel anti-malware

Pirates sur Snapchat :

En 2014, le service de partage de photos Snapchat s'est mis à dos les pirates informatiques après que la société ait déclaré n'avoir connaissance d'aucune vulnérabilité. Afin de prouver l'existence de ces failles, des pirates ont volé les noms d'utilisateur et les numéros de téléphone de 4,6 millions d'utilisateurs de Snapchat et les ont publiés sur un site Internet public. Même si le site a immédiatement été fermé et que Snapchat a déclaré avoir mis à jour ses mesures de sécurité en conséquence, l'incident a soulevé plusieurs questions importantes à propos de la confidentialité sur les réseaux sociaux : si les entreprises abandonnent leurs responsabilités, comment les familles se protégeront-elles ?

Qu'est-ce que Snapchat

Le but de Snapchat est simple : prendre une photo, l'envoyer à un ami et l'image disparaît au bout de 10 secondes. La problématique ? Il est possible de faire une capture d'écran d'une image avant qu'elle ne disparaisse ou de la récupérer depuis un appareil Android, même après sa suppression. Qui plus est, la propre politique de confidentialité de Snapchat stipule que les parents n'auront pas accès aux messages de leurs enfants. Pour trouver des amis sur Snapchat, les utilisateurs doivent saisir et confirmer leur numéro de téléphone. Le numéro de téléphone et le nom d'utilisateur : voilà ce qui a fait l'objet du récent piratage de Snapchat. Heureusement, il existe des moyens de protéger votre identité en ligne, même sur Snapchat.

Étape 1 : Changez de numéro de téléphone

Si le numéro d'un membre de votre famille a été publié dans la base de données des pirates, contactez votre opérateur et demandez qu'il vous attribue un nouveau numéro. Le fait de mentionner le piratage de Snapchat agira probablement en votre faveur, et vous pourrez peut-être obtenir un nouveau numéro gratuitement. Snapchat a également changé ses règles, en permettant aux utilisateurs de désactiver l'option « Trouver des amis », qui nécessite leur numéro de téléphone. Pour plus de sécurité, assurez-vous que cette option soit toujours désactivée.

Étape 2 : Modifiez votre mot de passe

Il est toujours bon de changer votre mot de passe de temps à autre, et c'est d'autant plus vrai après le piratage de Snapchat. Même si aucun membre de votre famille n'a été affecté, il n'est jamais superflu d'utiliser un mot de passe plus complexe. Votre meilleure carte pour assurer votre protection ? Choisissez une suite de mots dont vous pouvez vous souvenir, mais qui ne sont pas généralement liés ; voyez-le comme une brève histoire contenant plusieurs mots clés. Vous pouvez également choisir un ensemble de lettres, à la fois en majuscule et en minuscule, de chiffres et de symboles qui sera difficile à deviner. Assurez-vous simplement de pouvoir vous souvenir de ce mot de passe. Enfin, envisagez d'utiliser un gestionnaire de mots de passe qui vous permettra de gérer tous vos mots de passe tout en offrant un niveau de chiffrement adéquat.

Étape 3 : Ne vous faites plus avoir

Vous pourriez recevoir un appel ou un e-mail d'une personne prétendant travailler pour Snapchat. Ce n'est pas le cas. En premier lieu, aucun réseau social ne vous contactera par téléphone, et bien que les entreprises vous demandent occasionnellement de leur faire part de vos commentaires sur Internet, elles ne vous demanderont jamais d'informations personnelles. Tout e-mail prétendant que votre compte a été compromis et qu'il faut que vous fournissiez des informations personnelles pour le « réactiver » est faux.

Étape 4 : Choisir le nom d'utilisateur adéquat

Les noms d'utilisateur ont fait partie des données publiées par les pirates de Snapchat. Associés aux numéros de téléphone, cela met quiconque utilisant son véritable nom (ou une partie de ce dernier) en danger. Dans l'idéal, les enfants doivent choisir des noms d'utilisateur qui n'ont rien à voir avec leur véritable nom, leur âge ou leur adresse. Ce faisant, même dans le cas d'une faille de sécurité totale, les noms d'utilisateur ne pourraient être reliés aux vraies personnes.

Étape 5 : Prenez des photos « intelligentes »

Comme nous vous l'avons indiqué, les photos sur Snapchat doivent disparaître de l'écran pour toujours, mais elles ne s'effacent pas toujours. Bien qu'il soit peu probable qu'un piratage à grande échelle à l'instar du piratage des noms d'utilisateur et des numéros de téléphone fasse remonter à la surface toutes les photos prises dans l'application, il suffit de faire une capture d'écran de la photo, puis de la diffuser massivement sur Internet pour qu'elle soit visible de tous. Pour lutter contre ce problème, les parents doivent fixer des règles strictes concernant la prise de photos et leur publication : rien d'identifiable, par exemple des adresses ou des noms d'établissements scolaires, et aucune photo ne doit être envoyée à des amis que l'enfant ne connaît pas dans le

monde réel. L'anonymat protège les familles tout en induisant en erreur ceux qui pensent à causer du tort.

La protection des enfants sur Internet porte désormais largement sur les réseaux sociaux, et Snapchat n'en est que l'exemple le plus récent. Outre les conseils que nous avons donnés, il est toujours bon pour les familles d'utiliser un logiciel antivirus mais non gratuit qui inclut des fonctions de contrôle parental simples à utiliser, même pour les appareils mobiles. Les pirates de Snapchat sont la preuve vivante qu'aucun réseau social n'est parfaitement sécurisé, mais en disposant des bases adéquates et d'une solution de sécurité mobile appropriée, les familles peuvent dormir sur leurs deux oreilles.

Le cyberharcèlement : le cybercrime du siècle

Auparavant, le harcèlement était un problème que l'on rencontrait principalement dans la cour de l'école. Ce n'est plus le cas. Le « cyberharcèlement » fait son entrée — un problème qui prend de plus en plus d'ampleur pour de nombreux établissements scolaires. Et sous ses pires formes, le cyberharcèlement peut effectivement s'apparenter à de la cybercriminalité.

Qu'est-ce que le cyberharcèlement ?

On parle de cyberharcèlement lorsqu'un adolescent, un préadolescent ou un enfant utilise un appareil informatique pour menacer, humilier ou harceler de quelle que manière que ce soit un autre enfant. Il peut utiliser un ordinateur portable, un smartphone ou une tablette, et cyberharceler via diverses plateformes, par exemple SMS, e-mails, réseaux sociaux, forums en ligne et espaces de discussion. Dotés d'un appareil Internet et d'une connexion, les cyberharceleurs peuvent faire des ravages chez leurs victimes à tout moment, et presque en tout lieu. Et étant donné que cet acte ne nécessite pas d'interactions en face à face comme cela est le cas pour le harcèlement « physique », il peut s'avérer difficile d'attraper les coupables dans les temps.

Exemples de cyberharcèlement

Le cyberharcèlement prend de nombreuses formes cruelles. Un harceleur peut envoyer un SMS ou un e-mail dans le but de menacer sa victime ou de se moquer d'elle. Dans les cas les plus malveillants, il peut pirater les comptes de messagerie ou de réseaux sociaux pour usurper l'identité de sa victime et l'embarrasser en postant des publications diffamatoires en son nom. Certains cyberharceleurs vont même jusqu'à créer un site Internet afin d'humilier la cible qu'ils ont choisie.

Les tendances en matière de cyberharcèlement tendent à varier selon le sexe. Par exemple, les garçons sont réputés pour menacer d'autres garçons avec violence physique, mais ils harcèlent les filles en leur faisant des avances sexuelles par SMS. Les filles, en revanche, peuvent révéler des secrets ou répandre des mensonges ou des rumeurs à propos d'autres filles pour se

venger d'abus ressentis. Certaines jouent le rôle des « méchantes filles » en faisant des remarques dissuadantes sur les réseaux sociaux et en excluant d'autres personnes des groupes en ligne.

D'où l'importance de suivre une initiation sur la sensibilisation des dangers de l'internet pour les ados & adultes, ainsi que de voir comment assurer la sécurité des enfants sur internet !

Les répercussions du cyberharcèlement

Pour les victimes, les effets du harcèlement, quelle qu'en soit la forme, peuvent aller de la colère et de la souffrance à la haine de soi et aux tendances suicidaires. Il n'est pas rare que les cibles de ces actes barbares développent une faible estime d'elles-mêmes, de l'anxiété, de la dépression et d'autres problèmes susceptibles d'altérer leur santé mentale et émotionnelle. Le cyberharcèlement peut avoir des répercussions encore plus grandes sur les victimes en raison des moyens employés. Par exemple, des informations sensibles partagées par e-mail peuvent être envoyées à une dizaine de camarades de classe, tandis que des photos embarrassantes peuvent parvenir à des milliers de personnes une fois publiées sur les réseaux sociaux.

Du cyberharcèlement à la cybercriminalité

Bien que les réglementations locales continuent d'évoluer dans le monde au développement rapide du réseautage social sur Internet, le cyberharcèlement peut passer au stade de cybercriminalité. En 2011, deux filles, l'une âgée de 11 ans et l'autre de 12, ont été accusées de cyberharcèlement et d'intrusion sur ordinateur au premier degré pour des crimes qu'elles auraient commis à l'encontre d'une autre jeune fille de 12 ans, qui s'est avérée être une ancienne amie. Le duo a été accusé d'avoir publié des messages et des photos sexuellement explicites sur le profil Facebook de la victime après avoir mis la main sur son mot de passe. Les deux accusées ont risqué jusqu'à 30 jours dans un centre de détention pour mineurs pour les crimes qu'elles auraient commis. Ce cas n'est qu'un simple exemple de la manière dont le cyberharcèlement peut se transformer en cybercriminalité enfreignant la réglementation en vigueur. Parallèlement, il souligne l'importance grandissante de la sécurité des enfants sur internet.

Mettre fin au cyberharcèlement

La meilleure défense contre le cyberharcèlement, c'est la prévention, et les parents peuvent jouer un rôle actif dans ce processus en surveillant les activités numériques de leur enfant. En plus de veiller sur les relations avec lesquelles vos enfants communiquent par téléphone et SMS, vous pouvez utiliser un logiciel de sécurité Internet pour bloquer l'accès à du contenu inapproprié en ligne. Plus important, parlez de cyberharcèlement avec vos enfants.

Veillez à ce qu'ils sachent qu'ils peuvent venir en parler, à vous, un enseignant, un conseiller ou quelqu'un d'autre en qui ils ont confiance. Plus vite ils en parleront, et plus vite quelqu'un pourra mettre fin au problème.

La cybercriminalité c'est quoi ?

Parmi les différents types de développeurs de programmes malveillants, les plus dangereux sont probablement les pirates et groupes de pirates informatiques qui créent des programmes malveillants à des fins criminelles spécifiques. Ces cybercriminels créent des virus informatiques et des cheval de Troie capables de :

- Dérober des codes d'accès de comptes bancaires
- Promouvoir des produits ou services sur les ordinateurs de leurs victimes
- Utiliser illégalement les ressources des ordinateurs infectés afin de développer et de lancer :
    - Des campagnes de spam
    - Des attaques contre des réseaux distribués (ou attaques DDoS)
- Des opérations de chantage

Qu'est-ce que la cybercriminalité et quels en sont les risques ?

Pour en savoir plus sur le mode opératoire des cybercriminels et sur les risques encourus par les victimes de leurs activités, cliquez sur les liens ci-dessous :

- Moyens employés par les spammeurs
- Attaques contre les réseaux distribués/DDoS
- Qu'est-ce qu'un botnet ?
- Appels et SMS payants
- Vol de monnaie électronique
- Vol d'informations bancaires en ligne
- Ransomware et cyberchantage
- Évolution des méthodes de diffusion des virus
- Attaques de virus contre un ordinateur ciblé

Comment vous protéger de la cybercriminalité ?

Compte tenu des innombrables techniques qu'emploient les cybercriminels pour s'attaquer aux ordinateurs et aux données des utilisateurs, des défenses multicouches sont nécessaires. Les solutions de protection contre les programmes malveillants qui allient la détection basée sur les signatures, l'analyse heuristique et les technologies de Cloud permettent de renforcer la protection de vos ordinateurs, appareils et données contre les menaces toujours plus sophistiquées.

Kaspersky Lab propose des produits multicouches réputés pour leur efficacité qui protègent les ordinateurs et appareils suivants contre la cybercriminalité :

- PC Windows /Mac Apple / Smartphones / Tablettes

Comment se protéger des courriers indésirables

Le terme « courrier indésirable », ou « spam », fait partie de la terminologie Internet depuis l'avènement de la messagerie électronique, mais de quoi s'agit-il exactement ? Au fond, le courrier indésirable est une forme de courrier non sollicité par le destinataire. Il s'agit généralement d'un seul message de nature publicitaire envoyé à une multitude de destinataires qui n'ont jamais accepté de recevoir ce type de message. Les méthodes les plus couramment utilisées par les spammeurs pour constituer leurs listes d'adresses de messagerie comprennent l'achat de listes d'adresses, le fait de piéger des utilisateurs par le biais de faux concours et de fausses offres gratuites pour qu'ils leur transmettent leurs informations, ou encore l'utilisation de programmes de collecte d'adresses électroniques qui extraient des adresses sur les sites Web.

Pourquoi les courriers indésirables sont bien plus qu'une simple nuisance

Il existe de nombreuses raisons d'éviter toute interaction avec des courriers indésirables, mais certains des scénarios les plus inquiétants comprennent la possibilité de vous exposer au risque d'usurpation d'identité ou de permettre à un pirate d'installer des virus et programmes malveillants sur votre ordinateur. Dans les pires situations, des faits auxquels vous avez participé sans même le savoir aux côtés du spammeur peuvent même vous être reprochés, comme la participation à des opérations de blanchiment d'argent ou le recel d'objets volés. La plupart du temps, la meilleure attitude à adopter face à un courrier indésirable est la suppression immédiate du message.

De manière générale, si vous souhaitez éviter les courriers indésirables, rappelez-vous que si quelque chose semble trop beau pour être vrai, c'est probablement une arnaque. Cela vous aidera à rester à l'écart des offres et concours peu crédibles.

Comment vous protéger des courriers indésirables

Bien que les courriers indésirables puissent être difficiles à éviter, vous pouvez réduire considérablement, voire éliminer, la quantité de spams envahissant votre boîte de réception en utilisant un logiciel anti-spam adapté. Grâce aux progrès réalisés en intelligence logicielle, de nombreux filtres anti-spam sont capables d'apprendre automatiquement à différencier les messages légitimes des courriers indésirables en nécessitant une intervention minime de l'utilisateur. Dans le cas où un filtre anti-spam ne parviendrait pas à détecter

un message indésirable, il suffit à l'utilisateur de « marquer » le message comme un courrier indésirable. Le filtre s'adapte alors à la nouvelle menace.

Par la mise en œuvre d'une protection globale de la sécurité sur Internet, vous pouvez réduire sensiblement les dangers liés aux courriers indésirables en vous assurant de les exclure de votre boîte de réception et d'autres dossiers de messagerie importants. Qui plus est, de nombreux logiciels de sécurité Internet fournissent aux utilisateurs une protection contre le phishing, qui peut se révéler utile lorsqu'un e-mail semble être sérieux, mais ne l'est pas. Étant donné que ces e-mails demandent souvent des identifiants de connexion à des services bancaires ou financiers, la protection contre le phishing est un élément fondamental de tout outil anti-spam.

L'intérêt des logiciels de sécurité groupés

Lors de la sélection d'un logiciel anti-spam, il est judicieux de choisir une solution associée à une protection antivirus car certains messages indésirables s'accompagnent de virus et d'autres programmes malveillants. En utilisant une seule plateforme logicielle, vous simplifiez largement le processus de sécurisation de votre ordinateur tout en améliorant la fiabilité de votre système. Bien qu'un logiciel anti-spam soit capable d'écarter les messages de vos boîtes de réception, le fait de posséder un programme antivirus performant vous évitera d'infecter votre ordinateur si, par mégarde, vous ouvrez un message indésirable.

En savoir plus sur le phishing :

Quiconque utilise une messagerie électronique peut être victime d'une escroquerie de type phishing. Vous ne connaissez pas bien le principe du phishing ? Voici le scénario le plus courant : vous ouvrez votre messagerie et soudain une alerte de votre banque apparaît dans votre boîte de réception. Lorsque vous cliquez sur le lien dans l'e-mail, vous êtes conduit à une page Web qui ressemble, plus ou moins, au site de votre banque, mais qui est en réalité conçue pour voler vos informations. L'alerte prétend qu'il y a un problème avec votre compte et vous demande de confirmer votre identifiant et votre mot de passe. Après avoir entré vos informations d'identification sur la page qui apparaît, vous êtes habituellement dirigé vers le véritable site de l'établissement pour saisir vos informations une deuxième fois. Comme vous avez été redirigé vers le véritable établissement, vous ne réalisez pas immédiatement que vos informations ont été volées.

Quelques mesures simples pour vous protéger du phishing

Le phishing consiste à tromper des victimes pour les convaincre de fournir leurs informations de connexion à divers types de comptes sensibles, tels que la messagerie électronique, les intranets d'entreprise et plus encore.

Même les utilisateurs prudents peuvent parfois avoir du mal à détecter une attaque de phishing.
Ces attaques deviennent de plus en plus sophistiquées au fil du temps et les pirates trouvent des moyens de personnaliser leurs arnaques et de présenter des messages très convaincants qui peuvent facilement tromper les internautes.

La première mesure à prendre pour vous protéger sur Internet est de faire preuve de bon sens lorsqu'on vous demande de transmettre des informations confidentielles. Lorsque vous recevez un message d'alerte de votre banque ou d'un autre grand établissement, ne cliquez jamais sur le lien d'alerte figurant dans cet e-mail. Ouvrez une fenêtre de navigateur et tapez l'adresse directement dans le champ de l'URL pour vous assurer que le site est réel.

Autre indicateur majeur qu'il s'agit d'un site de phishing : le message comporte des fautes de frappe ou de langue et le site ne présente pas un aspect professionnel. Parce que les pirates mettent souvent en place leurs sites de phishing dans l'urgence, certains d'entre eux présentent un aspect très différent de celui de l'entreprise d'origine.

Logiciel de sécurité Internet pour une meilleure défense

L'une des manières les plus simples de vous protéger contre les tentatives de phishing consiste à installer et utiliser un logiciel de sécurité Internet adapté sur votre ordinateur. Un logiciel de sécurité Internet est vital à n'importe quel utilisateur, car il offre plusieurs couches de protection sous la forme d'une plateforme simple à gérer. En conjuguant pare-feu, protection anti-spam et protection anti-programmes malveillants dans un seul et même produit, il vous permet de réaliser des sauvegardes supplémentaires et vous évite ainsi de compromettre votre système si vous cliquez accidentellement sur un lien dangereux.

Un logiciel anti-spam est conçu pour protéger votre compte de messagerie contre le phishing et les courriers indésirables. Outre le fait qu'il s'appuie sur des listes noires prédéfinies créées par des chercheurs en sécurité, un logiciel anti-spam intègre une intelligence grâce à laquelle il « apprend » au fil du temps quels éléments sont indésirables et quels éléments ne le sont pas. Ainsi, bien que vous deviez continuer à faire preuve de vigilance, vous ressentirez une certaine sérénité à savoir que le logiciel filtre également les problèmes potentiels.

Un logiciel anti-programmes malveillants est inclus afin d'empêcher d'autres types de menaces. Semblable au logiciel anti-spam, le logiciel anti-programmes malveillants est programmé par des chercheurs en sécurité pour déceler les plus furtifs des programmes malveillants. Grâce à des mises à jour permanentes du fournisseur, le logiciel devient de plus en plus intelligent et à même de traiter les menaces les plus récentes. L'utilisation d'une solution anti-programmes malveillants gratuite vous protège des virus, des chevaux de Troie, des vers, etc.

Dans un contexte où la technologie évolue sans cesse, vous pouvez vous protéger contre le phishing et les autres menaces des programmes malveillants en utilisant une solution de sécurité développée par un fournisseur de sécurité réputé.

Quelle différence entre un logiciel antivirus et un logiciel contre les malwares ?

Les logiciels antivirus sont avant tout conçus pour prévenir les infections, mais offrent également la possibilité de supprimer les programmes malveillants d'un ordinateur infecté. Un logiciel de suppression des programmes malveillants autonome permet de détecter et de supprimer les programmes malveillants d'un ordinateur ou d'un appareil lorsque le produit déjà installé n'est pas en mesure de s'en charger.
Étant donné que l'achat d'un ordinateur représente l'un des investissements les plus conséquents d'un foyer ou d'une entreprise, il s'avère essentiel de le protéger contre les virus.

Bien que l'exécution d'une analyse antivirus joue un rôle essentiel dans la protection de votre ordinateur, les logiciels de suppression des programmes malveillants s'avèrent également nécessaires pour protéger votre ordinateur de manière optimale contre les divers virus et autres types de menaces. L'utilisation combinée d'un logiciel antivirus et d'un logiciel de suppression des programmes malveillants peut constituer la meilleure protection possible contre les programmes malveillants et les autres formes de menaces.

Logiciel antivirus ou logiciel de suppression des programmes malveillants : une différence majeure

Un logiciel antivirus sert avant tout à prévenir. le téléchargement des fichiers contenant des virus sur votre ordinateur. Il empêche également leur activation, en cas de téléchargement sur votre ordinateur et de placement dans la mémoire ou dans un fichier. Si le fichier infecté n'est pas téléchargé, aucun problème. S'il l'est, mais que le logiciel antivirus le signale en tant que programme malveillant et l'empêche d'être activé, votre système ne sera pas endommagé — même si le fichier infecté doit malgré tout être contrôlé et supprimé.

Quand doit-on utiliser un logiciel de suppression des programmes malveillants ?

Supposons qu'un fichier infecté soit téléchargé puis exécuté, activant ainsi le virus. Cela se produit généralement de manière accidentelle, notamment après avoir cliqué sur un lien URL corrompu ou ouvert une pièce jointe infectée dans un e-mail.

Certains logiciels antivirus peuvent inclure des outils rudimentaires permettant de supprimer des virus actifs, mais les programmes malveillants actuels sont sophistiqués. Ils se dissimulent dans l'ordinateur infecté et peuvent être réactivés ultérieurement. Par conséquent, ces outils rudimentaires peuvent s'avérer partiellement inefficaces.

Les logiciels de suppression des programmes malveillants proposent des outils spécifiquement conçus pour supprimer ces programmes d'un ordinateur infecté, dans l'éventualité où un virus échapperait à la vérification d'un logiciel antivirus. Les programmes malveillants comprennent des virus actifs, des virus contrôlés et des programmes malveillants inactifs pouvant être dissimulés dans l'ordinateur infecté.

Logiciels antivirus et de suppression des programmes malveillants, une protection intelligente

Les outils de suppression des programmes malveillants supplémentaires sont nécessaires parce que ces programmes peuvent se cacher, réapparaître, se propager et réinfecter le système, même si un fichier identifié contenant un virus est signalé et supprimé par le programme antivirus.

Les programmes malveillants peuvent exister sous différentes formes : fichier, fichier masqué ou partiellement corrompu ; ils peuvent dissimuler les mécanismes d'activation du virus, notamment en termes de lancement ou d'élément du registre. Dans le pire des cas, le programme malveillant fonctionne pour un tiers qui cherche à dérober des informations précieuses telles que des numéros de compte bancaire ou des identifiants personnels sans attirer l'attention. Avec les programmes malveillants modernes, la suppression d'un seul fichier infecté ne suffit généralement pas. Mieux vaut exécuter des vérifications dans plusieurs emplacements et utiliser des techniques d'analyse de virus pour supprimer complètement le programme malveillant.

De nombreuses offres gratuites d'antivirus et de détection des programmes malveillants sont disponibles et peuvent s'avérer très précieuses au départ si vous mettez en œuvre des mesures de sécurité sur vos ordinateurs personnels. Certains outils gratuits peuvent signaler si votre ordinateur est infecté et vous fournir un rapport complet des résultats, mais ils ne sont peut-être pas en mesure de supprimer les virus identifiés. Vous souhaiterez donc en définitive acheter un logiciel antivirus et un logiciel de suppression des programmes malveillants pour préserver efficacement votre investissement informatique.