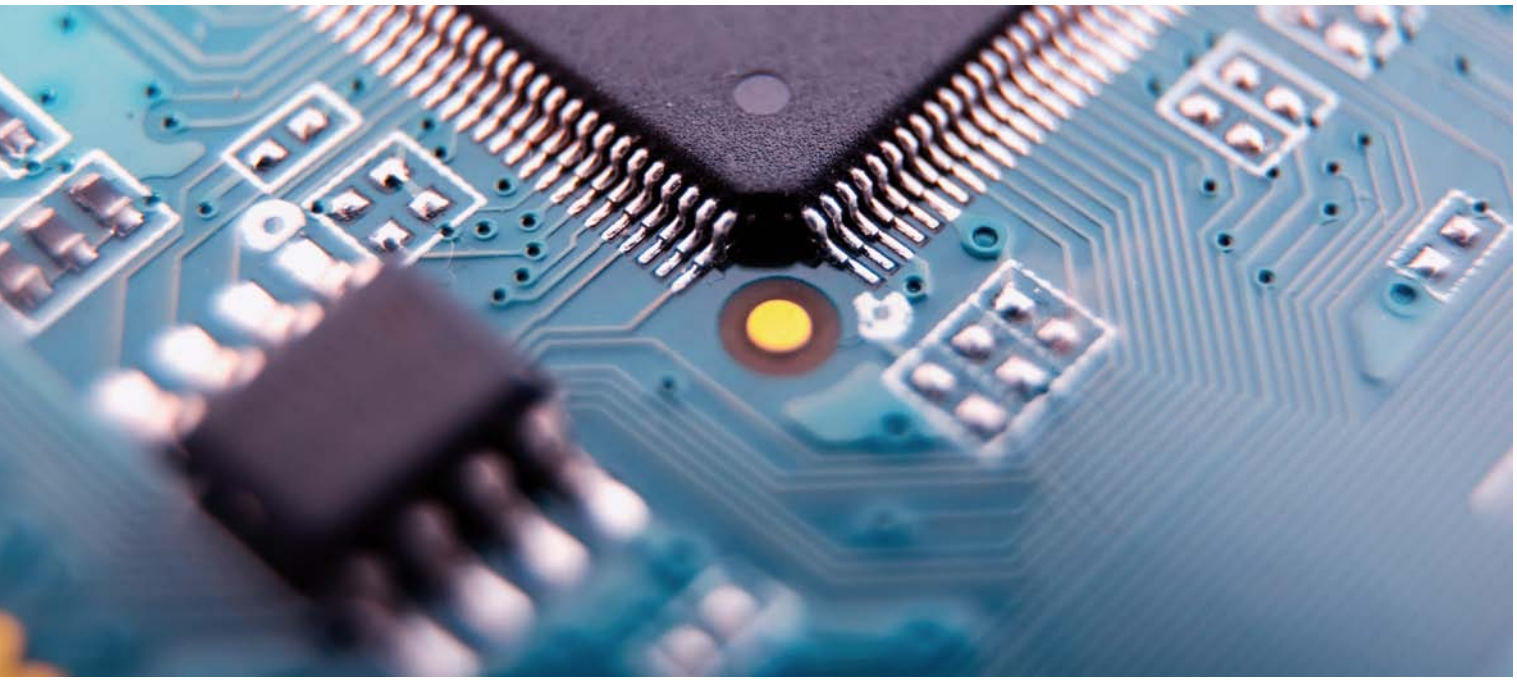
CREDIT SUISSE

La cybersécurité et vous

Sommaire

Cybersécurité



Pour Credit Suisse, la sécurité de vos données est primordiale. Aussi nous engageons-nous à protéger nos systèmes, nos logiciels, nos réseaux et nos autres ressources technologiques contre des personnes non autorisées cherchant à accéder aux données confidentielles ou à les détruire, à perturber nos services ou à causer d'autres dommages.

Nous disposons dans le monde entier de collaborateurs qui soutiennent nos efforts dans le domaine de la cybersécurité et qui travaillent notamment avec les autorités de réglementation, les forces de l'ordre et d'autres entreprises pour assurer notre protection et améliorer notre résistance aux menaces.

La technologie évolue rapidement dans un monde régi par les réseaux sociaux, les transactions en ligne, le cloud computing et les processus automatisés. Mais le progrès technologique s'accompagne aussi d'une montée de la **cybercriminalité**, dont les acteurs élaborent en permanence de nouveaux types d'attaque, des outils et des techniques qui leur permettent de pénétrer dans des environnements extrêmement complexes ou bien contrôlés, et de causer des dommages de plus en plus importants tout en restant intraçables.

Comme Internet fait probablement partie intégrante de votre vie, la cybercriminalité constitue une menace sérieuse et grandissante. Il est donc **indispensable** que nous intégrions tous consciemment la prévention de la fraude dans nos activités quotidiennes.

Face à la cybercriminalité, la présente brochure a pour objectif de vous rappeler comment vous protéger personnellement, ainsi que vos actifs et vos données sensibles.

Check-list de la cybersécurité

Quelques rappels pour protéger vos ordinateurs et votre argent des cybercriminels

1.
Faites tourner des logiciels de sécurité sur votre ordinateur et mettez-les à jour régulièrement pour qu'ils détectent les nouvelles menaces. Installez un antivirus pour vous protéger des programmes malveillants (malware) qui peuvent vous voler des données telles que des numéros de compte et des mots de passe, et utilisez un pare-feu pour empêcher tout accès non autorisé à votre ordinateur.

2.
Lorsque vous vous connectez à Internet pour accéder à votre relation bancaire ou effectuer des communications impliquant des données personnelles sensibles, prêtez attention au lieu où vous vous trouvez et à la façon dont vous procédez. Les réseaux Wi-Fi et les ordinateurs dans des lieux publics tels que des bibliothèques ou des centres d'affaires d'hôtel peuvent comporter des risques s'ils ne sont pas protégés par des logiciels de sécurité à jour.

3.
Familiarisez-vous avec les dispositifs de sécurité standard sur Internet. Installez un antivirus pour vous protéger des logiciels malveillants (malware) qui peuvent vous voler des données telles que des numéros de compte et des mots de passe, et utilisez un pare-feu pour empêcher tout accès non autorisé à votre ordinateur.

4.
Ignorez les e-mails non sollicités vous demandant d'ouvrir une pièce jointe ou de cliquer sur un lien si vous ne savez pas précisément qui vous les a envoyés ni dans quel but. Les cybercriminels excellent dans l'art de créer de faux e-mails qui ressemblent à des vrais, mais qui peuvent installer un logiciel malveillant. La meilleure approche à adopter est d'ignorer les messages non sollicités qui vous demandent d'ouvrir des pièces jointes ou des fichiers, ou de vérifier par vous-même que le prétendu expéditeur vous a bel et bien envoyé le message en question en le contactant via une adresse e-mail ou un numéro de téléphone officiels.

5.
Méfiez-vous si quelqu'un vous contacte en ligne de façon inattendue pour vous demander des données personnelles. Il est prudent d'ignorer les demandes d'informations non sollicitées, aussi légitimes qu'elles puissent paraître, en particulier si vous devez fournir des données telles qu'un numéro de sécurité sociale, des numéros de compte bancaire ou des mots de passe.

6.
Utilisez la procédure la plus sûre possible pour vous connecter à vos comptes financiers. Créez des mots de passe «solides» difficilentà percer, changez-les régulièrement et essayez de ne pas utiliser le même mot de passe ou le même NIP (numéro d'identification personnel) pour plusieurs comptes.

7.
Faites preuve de discrétion lorsque vous utilisez des sites de réseaux sociaux. Les criminels passent ces sites au crible pour trouver des informations telles que le lieu de naissance de quelqu'un, le nom de jeune fille de leur mère ou le nom d'un animal domestique qui pourront les aider à deviner ou à réinitialiser des mots de passe donnant accès à des comptes en ligne.

8.
Soyez prudent avec votre smartphone ou votre tablette. Ne laissez pas votre appareil mobile sans surveillance, et protégez-le par un mot de passe ou un autre moyen afin d'en interdire l'utilisation au cas où il serait volé ou perdu.

La cybersécurité personnelle en bref

Protégez votre ordinateur.

Installez un logiciel vous protégeant des programmes malveillants qui peuvent accéder à votre système sans votre accord pour y voler des mots de passe ou des numéros de compte. Utilisez également un pare-feu pour interdire tout accès non autorisé à votre ordinateur. Comme les systèmes de protection ont des fonctionnalités très diverses, assurez-vous que celles-ci permettent des mises à jour automatiques.

Recourez au mode de connexion le plus sûr pour vous connecter à vos comptes financiers.

Utilisez la procédure d'authentification la plus sûre du marché, en particulier pour les transactions à haut risque. Employez des mots de passe difficiles à percer et gardez-les pour vous. Créez des identifiants et des mots de passe «solides» pour vos ordinateurs, vos appareils mobiles et vos comptes en ligne en associant des majuscules et des minuscules, des chiffres et des symboles qu'il est difficile de deviner, et changez-les régulièrement. Bien qu'il soit tentant d'utiliser le même mot de passe ou le même NIP pour plusieurs comptes, vous risquez ainsi de permettre à un cybercriminel qui le perce d'accéder à tous ces comptes.

Familiarisez-vous avec les paramètres de sécurité d'Internet.

Vous pouvez avoir une plus grande assurance qu'un site web est authentique et qu'il crypte (brouille) vos données pendant leur transmission si son adresse commence par «https://». Vérifiez également que vous vous déconnectez correctement de vos comptes financiers lorsque vous avez achevé vos transactions ou que vous vous éloignez de votre ordinateur. Pour en savoir plus sur les mesures de sécurité supplémentaires, veuillez lire les instructions de votre navigateur Internet.

Méfiez-vous des e-mails non sollicités

Méfiez-vous des e-mails non sollicités qui vous demandent de cliquer sur un lien, de télécharger une pièce jointe ou de donner des informations sur un compte. Il est facile pour un cybercriminel de copier le logo d'une société ou d'une organisation renommée dans un e-mail d'hameçonnage (phishing). En répondant à une requête simple, il se peut que vous installiez un logiciel malveillant. La stratégie la plus sûre consiste à ignorer les demandes non sollicitées, aussi légitimes ou tentantes qu'elles puissent paraître.

Lorsque vous vous connectez à Internet, faites attention au lieu où vous vous trouvez et à la manière dont vous procédez.

Pour réaliser des opérations bancaires ou d'autres activités impliquant la saisie de données personnelles, accédez à Internet uniquement avec votre propre ordinateur portable ou appareil mobile au moyen d'une connexion connue et sûre en laquelle vous avez confiance. Un ordinateur public, comme on en trouve dans les centres d'affaires des hôtels ou dans les bibliothèques, et les réseaux Wi-Fi gratuits n'offrent pas forcément les garanties de sécurité requises. Il peut être relativement facile pour un cybercriminel d'intercepter le trafic Internet dans ce genre de lieu..

Soyez prudents lorsque vous utilisez des sites de réseaux sociaux.

Les cybercriminels se servent des sites de réseaux sociaux pour obtenir des informations sur des individus telles que leur lieu ou leur date de naissance, le nom de leur animal domestique, le nom de jeune fille de leur mère, ou tout autre renseignement pouvant les aider à percer des mots de passe ou à les réinitialiser. Ne communiquez pas votre «page» ou l'accès à vos données à quelqu'un que vous ne connaissez pas ou en qui vous n'avez pas confiance. Un cybercriminel peut prétendre être votre «ami» pour vous convaincre de lui envoyer de l'argent ou de divulguer des informations personnelles.

Prenez des précautions avec votre tablette ou votre smartphone.

Optez pour des mises à jour automatiques du système opérationnel et des applications de vos appareils dès qu'elles sont disponibles afin de réduire votre vulnérabilité aux problèmes de logiciel. Ne laissez jamais votre téléphone mobile sans surveillance et utilisez un mot de passe ou un autre paramètre de sécurité ordinapour en interdire l'accès au cas où il serait perdu ou volé. Veillez à activer la fonction «time out» (délai d'extinction automatique) ou «autolock» (autoblocage) lorsque vous ne l'utilisez pas pendant un certain temps. Faites des recherches sur les nouvelles applications avant de les télécharger.

La cybersécurité de l'entreprise en bref

Protégez les ordinateurs et les réseaux.

Installez des logiciels de sécurité et d'antivirus qui vous protègent des programmes malveillants (malware) susceptibles d'accéder à un système informatique sans l'accord de son propriétaire dans le but notamment de voler des données. Utilisez également un pare-feu pour interdire tout accès non autorisé. Comme les options de protection sont nombreuses, choisissez-en une qui soit adaptée à la taille et à la complexité de votre entreprise. Procédez à des mises à jour selon les besoins, de sorte que vos logiciels restent efficaces. Par exemple, paramétrez un antivirus pour qu'il lance un scan après chaque mise à jour. Si vous recourez à un réseau sans fil (Wi-Fi), veillez à ce qu'il soit sécurisé et crypté. Protégez l'accès au routeur au moyen de solides mots de passe.

Exigez une procédure d'authentification rigoureuse.

Veillez à ce que les collaborateurs et d'autres utilisateurs qui se connectent à votre réseau utilisent des identifiants et des mots de passe complexes pour les ordinateurs, les appareils mobiles et les comptes en ligne en associant des majuscules et des minuscules, des chiffres et des symboles difficiles à deviner, et à ce qu'ils les changent régulièrement. Pensez à implémenter un mode d'authentification multi-facteurs qui requiert des informations supplémentaires en dehors d'un mot de passe avant d'autoriser un accès. Assurez- vous auprès de vos fournisseurs traitant des données sensibles qu'ils appliquent un système d'authentification multi-facteurs pour accéder à des systèmes ou à des comptes.

Contrôlez l'accès aux données et aux ordinateurs.

Contrôlez l'accès aux données et aux ordinateurs et créez un compte utilisateur pour chaque collaborateur. Prenez des mesures pour limiter aux personnes autorisées l'accès aux ordinateurs de l'entreprise ou leur utilisation. Bloquez les ordinateurs portables lorsqu'ils ne sont pas employés, car ils peuvent être facilement volés ou perdus. Exigez que chaque collaborateur ait un compte utilisateur séparé et interdisez que des comptes soient partagés. Faites en sorte que les collaborateurs aient seulement accès aux systèmes de données spécifiques dont ils ont besoin pour leur travail, et ne les laissez pas installer des logiciels sans autorisation. Veillez également à ce que seuls les collaborateurs bénéficiant de privilèges administratifs, tels que les spécialistes informatiques et les membres du personnel clé, aient ces accès et que leurs besoins à cet égard soient régulièrement examinés.

Enseignez les règles de base à vos collaborateurs.

Établissez des pratiques en matière de sécurité et des directives correspondantes pour les collaborateurs, telles qu'un guide d'utilisation d'Internet, et définissez des attentes mais aussi des sanctions en cas de violation des dispositions imposées. Mettez en place une culture d'entreprise pyramidale qui rappelle l'importance d'une solide cybersécurité, en particulier lorsqu'il s'agit de traiter et de protéger les données des clients et d'autres informations stratégiques. Veillez à ce que tous les collaborateurs sachent comment identifier et signaler de possibles incidents touchant à la sécurité. Formez-les pour qu'ils soient attentifs au lieu où ils se connectent à Internet et à la manière dont ils le font. Les collaborateurs et des tiers devraient accéder à votre réseau en utilisant uniquement une connexion sûre et fiable, ce qui n'est pas forcément le cas des ordinateurs publics que l'on trouve par exemple dans un cybercafé, le centre d'affaires d'un hôtel ou une bibliothèque publique. De même, vos collaborateurs ne devraient pas accéder au réseau de votre entreprise s'ils ne sont pas sûrs de la connexion sans fil qu'ils utilisent, notamment lorsque plusieurs réseaux Wi-Fi gratuits sont mis à disposition dans des points d'accès (hotspots) publics. Dans de tels endroits, il peut être relativement facile pour un cybercriminel d'intercepter le trafic Internet.

Prévenez vos collaborateurs des dangers que présentent les e-mails suspects.

Les collaborateurs doivent se méfier des e-mails non sollicités qui leur demandent de cliquer sur un lien, d'ouvrir une pièce jointe ou de fournir des informations sur un compte. Un cybercriminel peut aisément copier le logo d'une entreprise ou d'une organisation renommée dans un e-mail d'hameçonnage (phishing). En répondant à ce qui semble être une simple requête, vos collaborateurs sont susceptibles d'introduire un programme malveillant dans votre réseau. La stratégie la plus sûre consiste à ignorer de telles demandes, aussi légitimes qu'elles puissent paraître. Les fournisseurs de logiciels procurent régulièrement des correctifs ou des mises à jour de leurs produits afin de remédier aux failles de sécurité et d'en améliorer les fonctionnalités. Il est judicieux de télécharger et d'installer ces mises à jour dès qu'elles sont disponibles. Il peut être encore plus efficace de configurer vos logiciels de telle manière qu'ils procèdent automatiquement à ces opérations.

Faites des copies de sauvegarde

Faites des copies de sauvegarde des systèmes et des informations importants. Sauvegardez régulièrement les données des ordinateurs utilisés au sein de votre entreprise. Veillez à appliquer les mêmes mesures de sécurité (p. ex. cryptage) aux copies etaux originaux. En dehors des sauvegardes automatiques, copiez régulièrement les données sensibles dans un périphérique de stockage conservé en lieu sûr sur un autre site.

Prêtez une attention particulière à vos comptes bancaires.

Prêtez une attention particulière à vos comptes bancaires et surveillez les retraits non autorisés. Mettez en place des contrôles supplémentaires, tels qu'un appel de confirmation, avant d'autoriser l'établissement financier à effectuer un virement. Ces dernières années, on a constaté une augmentation du nombre de transferts électroniques non autorisés émanant de comptes bancaires d'entreprises. Le piratage de compte est fréquent: les cybercriminels se servent d'un logiciel malveillant tel qu'un enregistreur de frappe (« key stroke logger ») pour obtenir les identifiants et les mots de passe de comptes bancaires en ligne et effectuer ensuite des retraits. Autre escroquerie possible: les attaques de messagerie en entreprise (Business Email Compromise/BEC), qui consistent à imiter les demandes de paiement de fournisseurs réels et à faire transférer les fonds sur le compte du cybercriminel. Or les entreprises ne sont généralement pas couvertes par la protection des consommateurs en ce qui concerne les transferts électroniques de fonds non autorisés.

N’oubliez pas les tablettes et les smartphones.

Les appareils mobiles peuvent être à l’origine de problèmes de sécurité, en particulier s’ils contiennent des informations confidentielles ou permettent d’accéder au réseau de votre entreprise. Si vos collaborateurs connectent leurs appareils à celui-ci, exigez qu’ils les protègent par un mot de passe, qu’ils cryptent leurs données et qu’ils installent des applications de sécurité afin d’éviter que des cybercriminels n’y accèdent lorsqu’ils sont connectés à des réseaux publics. Veillez à définir et à appliquer des procédures de notification en cas de vol ou de perte de tels équipements.

Méfiez-vous des transactions et des factures frauduleuses.

Les escroqueries prennent toutes sortes de formes: paiement avec un chèque sans valeur, fausse carte de crédit ou de débit, retour frauduleux de marchandise, etc. Assurez-vous contre ces risques et faites en sorte de signaler immédiatement toute irrégularité.

E-mail

Les fournisseurs d'e-mail ne peuvent pas garantir votre cybersécurité, et les pirates les attaquent pour accéder à vos comptes. Ils peuvent également s'en prendre directement aux comptes e-mail individuels en recourant à l'hameçonnage, à l'ingénierie sociale, aux logiciels malveillants et à d'autres moyens frauduleux.

Limitez vos risques en tenant des comptes e-mail séparés pour:

- votre activité professionnelle,
- vos amis et votre famille,
- les alertes importantes, les sites exigeant une adresse e-mail comme identifiant

En outre, pour la sauvegarde de vos données:

- paramétrez, si possible, une authentification à deux facteurs dans votre service e-mail pour recevoir un avertissement lorsqu'un autre ordinateur s'y connecte;
- recourez au cryptage lorsque vous envoyez des données personnelles. L'encodage empêche les personnes ne possédant pas les clés de déchiffrage de lire les informations transmises;
- utilisez des filtres anti-spam pour réduire le risque de recevoir des logiciels malveillants ou des messages d'hameçonnage (les spams représentent 65% des échanges d'e-mails);
- si vous devez envoyer à quelqu'un un document protégé par un mot de passe, envoyez le dans un premier e-mail et le mot de passe dans un second.

Ingénierie sociale

L'ingénierie sociale peut vous rendre vulnérable aux escrocs. Les médias sociaux tels que Facebook ou LinkedIn peuvent permettre aux pirates d'obtenir une mine d'informations sur vous et de les utiliser ensuite pour vous voler des actifs ou des données.

- Limitez les informations que vous postez en ligne. Les criminels recherchent dans Facebook, Twitter et dans d'autres médias sociaux des informations vous concernant afin de vous tromper, ainsi que votre famille et/ou vos amis.
- Ne communiquez pas de données personnelles/ financières par e-mail (et ne suivez pas des liens reçus par e-mail, même s'ils proviennent de sources fiables).
- Téléphonez à l'expéditeur de l'e-mail ou créez un nouveau message (ne cliquez pas sur «répondre») pour lui demander si l'e-mail qu'il a envoyé émane réellement de lui.
- Faites attention à l'URL. Les sites Internet malveillants semblent identiques aux vrais, mais l'URL peut contenir une variante orthographique ou un domaine différent (p. ex. se terminer par .net au lieu de .com).
- Ne saisissez des données sensibles dans un site web que si vous voyez qu'il est sécurisé (l'URL devrait commencer par: https//).

Au téléphone

Faites-vous confirmer l'identité de l'appelant si celui-ci vous est inconnu: demandez-lui de vous épeler l'intégralité de son nom, d'indiquer un numéro de rappel et d'expliquer pourquoi il a besoin des informations qu'il demande.

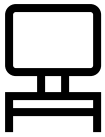
Méfiez-vous des imposteurs: faites-vous confirmer la source de l'appel par des canaux publics officiels.

Ne fournissez pas d'informations sur des tiers: dites à l'appelant de contacter directement la personne concernée s'il vous demande des informations à son sujet.

En personne

Dans des lieux publics, faites preuve de vigilance car des personnes peuvent observer par-dessus votre épaule les données personnelles que vous saisissez (telles qu'un NIP ou un mot de passe) afin de les utiliser pour accéder à vos comptes.

- Méfiez-vous des personnes qui tentent d'entrer dans une zone sécurisée sans présenter d'autorisation telle qu'un badge ou un jeton de sécurité.
- N'insérez pas dans votre ordinateur un support de stockage amovible (p. ex. clé USB) que vous avez trouvé ou qui vous a été donné, car il peut contenir un logiciel malveillant.



Internet

Les pirates parviennent à recréer des sites Internet connus pour capturer vos éléments d'authentification tels que mot de passe, numéro de sécurité sociale, informations sur vos cartes de crédit. Ils les utilisent ensuite pour accéder à vos comptes bancaires ou à d'autres comptes.

Précautions à prendre en ligne:

- Veillez à ce que votre navigateur soit à jour.
- Paramétrez votre navigateur pour maintenir un niveau de sécurité moyen ou élevé.
- Assurez-vous que l'adresse web de tous les sites que vous consultez commence par « https:// ». Certains navigateurs affichent l'icône d'un cadenas à côté de l'adresse « https:// » pour indiquer que la connexion est sécurisée.
- Souvenez-vous: une adresse « http:// » n'est pas sécurisée.
- Déconnectez-vous après avoir utilisé des services bancaires et d'e-commerce sur Internet pour vous assurer que votre session est bien fermée.
- Effacez les cookies et la mémoire cache de votre navigateur de façon que les pirates ne puissent pas accéder à votre historique de navigation et obtenir ainsi des informations.
- Souvenez-vous que les pirates ciblent de plus en plus les enfants sur les sites de médias sociaux et de jeux.
- Faites attention aux sites que vous visitez: ne consultez pas ceux qui proposent des téléchargements ou des contenus illégaux (p. ex. partage de fichiers), car même si vous ne téléchargez rien, vous vous exposez à des virus susceptibles d'infecter votre ordinateur.
- Bloquez les pop-ups (fenêtres contextuelles) et la publicité, et ne répondez jamais à des pop-ups vous demandant de saisir ou de ressaisir vos données de connexion.

Meilleure pratique

- Vérifiez régulièrement si vos historiques et relevés de transactions bancaires et de cartes de crédit ne contiennent pas des opérations suspectes.
- Utilisez si possible l'authentification à deux facteurs (vous confirmez votre identité en deux étapes lorsque vous utilisez un guichet automatique de banque) avec votre carte de débit et votre NIP. Faites de même en ligne: pour accéder à votre compte, entrez un mot de passe et un code qui vous est communiqué par un texto, un e-mail ou un appel téléphonique. Vous recevrez une alerte si quelqu'un se connecte à partir d'un autre ordinateur.
- Évitez de cliquer sur le bouton «fermer» d'une publicité ou à un autre endroit dans sa fenêtre pour la faire disparaître.
- Dans la mesure du possible, activez la navigation privée pour éviter que des cookies ou un historique de navigation ne soient stockés ou enregistrés sur votre ordinateur.
- Utilisez des signets fiables pour les sites importants (ni liens e-mail, ni pop-ups).
- Fermez les fenêtres contenant des pop-ups de publicité ou des alertes inattendues en cliquant sur le X figurant dans l'angle supérieur droit.
- N'achetez aucun article proposé par un spam, même si celui-ci provient d'une société connue, car votre achat encouragera l'envoi de ces messages indésirables.

Souvenez-vous que tous les appareils comportent des risques.

Les ordinateurs portables, les tablettes et les téléphones mobiles peuvent tous faire l'objet d'atteintes à la sécurité des données. Ne vous connectez pas à des sites que vous ne connaissez ou ne reconnaissez pas. Ne présumez pas qu'une connexion Wi-Fi est fiable; les pirates créent des points d'accès qui semblent être identiques aux connexions valides. Utilisez plutôt un réseau privé virtuel (VPN) qui donne accès uniquement aux utilisateurs autorisés afin que les données ne puissent pas être interceptées.

Sécurité mobile

Nous dépendons de plus en plus de nos smartphones et de nos tablettes pour nos opérations bancaires, nos achats et nos relations sociales. Il est donc indispensable de les protéger. Nous devrions tous prendre des précautions dans ce sens.

Meilleures pratiques pour vos appareils personnels

- Ajustez vos paramètres de sécurité pour que des tiers ne puissent pas accéder à vos données via des connexions sans fil ou Bluetooth.
- Évitez de cliquer sur des publicités sur Internet: il existe des applications permettant le blocage de publicités sur les appareils Android et Apple, et il est possible d'ajuster les paramètres du navigateur pour limiter le suivi de publicités.
- Mettez à jour les applications sur votre appareil dès que de nouvelles versions sont disponibles, car celles-ci comportent souvent des correctifs de sécurité.
- Si vous pensez que votre appareil a été infecté par un logiciel malveillant, demandez de l'aide à son fabricant ou à votre opérateur de téléphonie mobile.
- Installez une application de sécurité pour scanner et éliminer les applications infectées par un logiciel malveillant.
- N'essayez pas de contourner les contrôles de sécurité du système d'exploitation de votre appareil (c.-à-d. ne déverrouillez pas votre téléphone ou ne le rootez pas).
- Laissez votre téléphone ou votre ordinateur bloqué. Veillez à ce qu'il soit toujours protégé par un mot de passe/NIP.
- Mettez à jour le logiciel d'exploitation de votre appareil et assurez-vous que vous disposez des correctifs de sécurité les plus récents.
- Cryptez les données sensibles. Si votre appareil mobile ou votre ordinateur portable est équipé de paramètres d'encodage, utilisez-les.
- Contrôlez comment les applications se comportent sur votre téléphone. Gardez la trace des demandes/autorisations d'accès émanant des applications installées sur votre appareil.
- Utilisez un programme reconnu de protection contre les logiciels malveillants/ virus et mettez-le à jour régulièrement. Vos appareils mobiles sont exposés aux mêmes risques que vos ordinateurs privés et professionnels.
- Fermez la connexion Bluetooth lorsque vous n'en avez pas besoin. Votre appareil sera ainsi moins exposé aux cyberattaques, et vous n'en déchargerez pas la batterie.
- Choisissez un smartphone équipé d'un système antivol. S'il est volé ou perdu, l'accès à distance vous permettra de le bloquer, d'effacer les données qu'il contient et de le localiser.
- Sauvegardez régulièrement les données de vos appareils sur votre ordinateur à domicile ou sur un cloud de façon à pouvoir y accéder si les appareils en question étaient perdus, volés ou endommagés.
- Les criminels utilisent des logiciels malveillants pour voler ou détruire des données, ce qui compromet la sécurité et l'intégrité des appareils et/ou des systèmes que vous utilisez. N'ignorez pas les avertissements. Installez un antivirus et surveillez les alertes que vous recevez, p. ex. lorsque vous essayez d'ouvrir un site dangereux sur Internet.
- Faites attention à ce que vous sélectionnez ou téléchargez. En cliquant sur des liens inconnus, vous pouvez vous exposer à des logiciels malveillants qui scannent votre ordinateur ou surveillent les touches actionnées, notamment en quête de mots de passe et de numéros de compte.
- Certains programmes comportent à dessein des logiciels malveillants. Lorsque vous les installez, surveillez les messages encadrés et les petits caractères. Annulez toute installation qui pourrait causer des dommages.
- Méfiez-vous des e-mails suspects. Même ceux provenant de vos connaissances peuvent contenir des pièces jointes ou des liens dangereux si leur propre compte a été compromis.
- Soyez prudent lorsqu'il s'agit de suivre un lien fourni par un e-mail entrant. Dans la mesure du possible, consultez le site Internet en question en saisissant son adresse directement dans votre navigateur.
- Scannez les fichiers avec votre logiciel de sécurité avant de les ouvrir. Ne présumez pas que les fichiers reçus par e-mail, sur un disque ou une clé USB sont sûrs.

Logiciels malveillants

Ne faites pas confiance aux pop-ups vous demandant de télécharger un logiciel. Leur objectif est de vous convaincre que votre ordinateur a été infecté et que l'installation du programme en question permettra de résoudre le problème. Fermez cette fenêtre immédiatement en veillant à ne pas cliquer sur quoi que ce soit se trouvant à l'intérieur.

- La plupart des sites de partage de fichiers sont illégaux et doivent être évités. Ils comportent très peu de contrôles de logiciels malveillants. Ces derniers peuvent prendre la forme d'un film à succès, d'un album ou d'un programme.
- Si votre ordinateur a été infecté par un virus visant à vous rançonner (ransomware), c'est-à-dire si un pop-up vous informe que vos fichiers ont été encodés et qu'ils seront décryptés en échange d'une rançon, ne paniquez pas. Déconnectez immédiatement votre appareil du réseau et essayez de restaurer vos fichiers à l'aide d'une sauvegarde antérieure. Ne payez pas la rançon.

CREDIT SUISSE AG
Case postale 100
CH-8070 Zurich
credit-suisse.com

MCIZ 02.2019