Vous êtes la cible

De nombreuses personnes croient à tort que leurs informations ou leur ordinateur n'ont aucune valeur, et qu'elles ne feront jamais l'objet de l'attaque de la part de cybercriminels. En réalité, les personnes comme vous sont des cibles principales des cybercriminels. Vous et votre ordinateur sont attaqués tous les jours. La première étape pour vous protéger consiste à comprendre que vous êtes leur cible.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse:
securite.informatique@lausanne.ch

Lausanne

Vous êtes la cible

L'une des choses les plus importantes à comprendre, c'est que vous êtes la cible. De nombreuses personnes croient à tort que les cybercriminels ne s'attaquent qu'à nos bases de données ou nos serveurs Internet. Vous êtes en réalité l'une des cibles principales des cybercriminels. Bien que ces agresseurs aient accès à de nombreux outils sophistiqués, pour eux, la manière la plus simple d'agresser une société est de cibler les personnes qui y travaillent, comme vous. Regardons comment un groupe de cybercriminels peut pirater notre organisation. Même si l'histoire suivante n'a pas réellement eu lieu, elle illustre des méthodes fréquemment utilisées pour pirater une organisation comme la nôtre.

Il y a plusieurs mois, un groupe de cybercriminels a décidé de cibler notre organisation. Nous ne savons pas vraiment quelle était leur motivation. Peut-être voulaient-ils voler nos informations sensibles, faire une déclaration politique ou accéder à l'un de nos partenaires. Tout ce que nous savons, c'est qu'il y a quelques semaines, ils ont commencé à chercher sur notre site tout ce qu'ils pouvaient apprendre sur nous. Cela incluait qui nous sommes, comment nous fonctionnons et les identités des employés et du personnel. Ils ont alors commencé à recueillir les données personnelles des employés à partir de sites Internet tels que Facebook, YouTube, LinkedIn, Instagram et des forums publics.

Malheureusement, plusieurs employés avaient posté trop d'informations sur eux-mêmes et notre organisation. En conséquence, les criminels ont réussi à construire une image complète de notre organisation et à apprendre des informations sur les membres clés de notre personnel. Armés de ces informations, ils ont lancé leur attaque. Sept employés de notre organisation ont reçu des courriels qui semblaient provenir d'un service de livraison de colis que nous utilisons couramment. Ces courriels qui semblaient être légitimes, étaient, en fait, une tentative de phishing créée par les criminels. Chaque message contenait une pièce jointe infectée conçue pour contourner notre logiciel anti-virus et infecter silencieusement nos ordinateurs.

Malheureusement, deux des employés ciblés ont été victimes des courriels d'hameçonnage en ouvrant les pièces jointes. Comme leurs ordinateurs n'étaient pas à jour, ils ont été rapidement infectés, donnant aux criminels un contrôle complet du système. Les criminels ont ensuite installé un logiciel enregistreur sur les ordinateurs, ce qui leur a permis de capturer toutes les frappes de clavier des employés. Sur l'un des ordinateurs piratés, un employé utilisait un identifiant et un mot de passe qui était partagés avec ses collègues. Les criminels ont récolté rapidement ces informations et ont pu se connecter à d'autres systèmes dans toute notre organisation. Dans la mesure où ils avaient volé des mots de passe légitimes, notre équipe de sécurité n'a pas détecté les criminels.

Au cours des sept jours suivants, les criminels ont scanné les disques durs de nombreux systèmes compromis, tout en volant chaque document, feuille de calcul et présentation qu'ils pouvaient trouver. Ils ont rapidement transféré plus de 150 giga-octets d'informations confidentielles sur notre organisation, y compris un projet clé sur lequel nous avions travaillé pendant plus de trois mois. Heureusement, un employé avisé a remarqué plusieurs programmes suspects en cours d'exécution sur son ordinateur et l'a signalé. En conséquence, les criminels ont finalement été identifiés et bloqués, les empêchant de causer plus de tort.

Vous êtes la cible

Bien que ce soit seulement un exemple fourni à titre d'illustration, cela démontre pourquoi nous avons mis en place des politiques et des contrôles de sécurité. Ces outils ont été spécifiquement conçus pour vous protéger et pour protéger notre organisation, tout en garantissant que nous nous conformons bien à toutes les normes et les réglementations importantes. C'est pourquoi il est tellement important que vous compreniez bien et que vous suiviez nos politiques en matière de sécurité.

Peut-être n'en êtes-vous pas conscient, mais vous êtes également menacé lorsque vous et votre famille vous connectez à Internet à la maison. Pour vous protéger, vous, votre famille et notre organisation, n'oubliez pas certains principes de base :

- Soyez toujours prudent et supposez que vous êtes une cible. Vous pensez peut-être que vous ou vos informations n'avez pas de valeur, mais ce n'est pas le cas.

- Les attaques sont une menace constante sur Internet. Si quelque chose vous semble suspect, ou trop beau pour être vrai, c'est sûrement le cas.

La cybercriminalité est extrêmement bien organisée

Au cours de la dernière décennie, les cybercriminels sont devenus extrêmement performants. À leurs débuts, les cybercriminels travaillaient souvent seuls. Ils devaient construire leurs propres outils d'attaque, trouver et pirater manuellement des ordinateurs, voler des détails bancaires et transférer par voie électronique les fonds ou les informations volés eux-mêmes. Les cybercriminels d'aujourd'hui sont beaucoup plus perfectionnés. Chaque criminel a maintenant son propre champ spécifique d'expertise ; et ensemble ils ont développé leur propre communauté hautement organisée. Un groupe est dédié par exemple au développement et à l'assistance des outils d'attaque innovants. Un autre groupe se spécialise dans le piratage d'autres ordinateurs ou le blanchiment de l'argent volé. C'est toute une économie basée sur la cybercriminalité qui se développe, elle améliore en permanence ses tactiques et se montre chaque jour plus efficace dans sa course au profit. Ces criminels forment une menace très performante, et cette menace nous poursuivra pendant de nombreuses années.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse: securite.informatique@lausanne.ch

Lausanne

Ingénierie sociale

Les cybercriminels ont appris que la façon la plus simple de prendre le contrôle de votre ordinateur ou de voler vos mots de passe est tout simplement de vous le demander. Faites preuve de bon sens. Si une personne ou un message vous semblent suspects, ou si cela semble trop beau pour être vrai, c'est peut-être une attaque.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse: securite.informatique@lausanne.ch

Lausanne

Ingénierie sociale

L'une des principales techniques que les cybercriminels utilisent pour prendre le contrôle de vos ordinateurs et voler vos informations est appelée l'ingénierie sociale, qui est également connue comme l'art de la manipulation humaine. Les criminels font alors semblant d'être une personne ou une entité que vous connaissez ou en qui vous avez confiance, comme votre banque, un organisme gouvernemental ou même un ami ou un collègue. Ils exploitent alors cette confiance pour obtenir ce qu'ils veulent, souvent en le demandant, tout simplement. Jetons un œil aux différents exemples d'attaques d'ingénierie sociale.

Email

Vous recevez un email provenant d'une société de livraison, indiquant que la société a tenté de vous livrer un colis mais qu'elle avait une adresse incorrecte. L'email semble officiel, il arbore des graphismes semblant professionnels et le logo d'une véritable entreprise. Cet email vous informe que si vous ne répondez pas dans les 24 heures suivantes, votre colis sera retourné à l'expéditeur. Il vous donne ensuite un lien sur lequel vous devez cliquer ou une pièce jointe à remplir pour recevoir votre colis. Le problème, c'est que c'est une attaque. Un cybercriminel a créé un email qui ressemble exactement à celui d'une véritable société de livraison ; cependant, cet email a été créé pour vous tromper. Si vous cliquez sur le lien, vous vous rendrez sur un site Internet contrôlé par le criminel. Une fois que votre navigateur sera connecté au site Internet du criminel, il va tenter de le pirater discrètement. Si vous ouvrez la pièce jointe, votre ordinateur sera infecté discrètement. Méfiez-vous des emails non attendus qui vous poussent à cliquer sur des liens ou à ouvrir des pièces jointes.

Arnaque à l'assistance informatique

Vous recevez un appel téléphonique de quelqu'un qui prétend provenir d'une entreprise d'assistance informatique. Les criminels disent qu'ils croient que votre ordinateur est infecté, qu'ils ont été chargé d'enquêter sur la question et de vous aider à sécuriser votre ordinateur. Par exemple, ils peuvent vous demander de trouver des fichiers spécifiques sur votre ordinateur et vous expliquer comment les trouver. Lorsque vous trouvez ces fichiers, votre interlocuteur vous expliquera que c'est un signe que votre ordinateur est infecté. C'est bien entendu un mensonge, votre ordinateur n'est pas infecté. En réalité, ces fichiers ne sont que des fichiers communs trouvés sur chaque ordinateur. Une fois qu'ils vous ont trompé en vous faisant croire que votre ordinateur est infecté, ils vont vous forcer à acheter leur logiciel de sécurité. Cependant, le logiciel qu'ils vendent n'est pas vraiment un logiciel de sécurité. Il s'agit en fait d'un programme infecté qui va leur donner le contrôle total de votre ordinateur. En fin de compte, non seulement vous ont-ils trompé en infectant votre ordinateur, mais vous les avez payés pour le faire.

Réseaux sociaux

Une amie poste un message sur sa page Facebook, qui dit qu'elle est à Londres et qu'elle s'est faite voler. Elle a besoin qu'on lui envoie immédiatement de l'argent pour rentrer. C'est un mensonge. Votre amie n'a

Ingénierie sociale

pas été volée, elle n'est même pas à Londres. C'est un cybercriminel qui a piraté son compte Facebook et qui a posté ce faux message pour dérober de l'argent à ses amis. Dans ce cas, la meilleure manière de vous protéger, c'est d'appeler cette amie au téléphone pour vérifier si elle a vraiment besoin d'aide.

Rappelez-vous, l'ingénierie sociale n'est rien de plus qu'un criminel qui construit une relation de confiance avec vous, avant d'abuser de cette confiance pour obtenir ce qu'il veut. Si vous recevez un courriel, un message ou un appel téléphonique qui semble bizarre, suspect ou trop beau pour être vrai, c'est peut-être une attaque. Les indicateurs communs d'une attaque d'ingénierie sociale comprennent des personnes qui demandent des informations auxquelles elles ne devraient pas avoir accès, à l'aide d'un grand nombre de termes ou de techniques prêtant à confusion ou en créant un sentiment d'urgence. Si vous pensez que quelqu'un tente de vous tromper, il suffit de raccrocher le téléphone ou d'ignorer le message et de communiquer immédiatement avec le service d'assistance ou l'équipe en charge de la sécurité des informations.

Vous avez gagné à la loterie

Vous recevez un SMS sur votre smartphone vous annonçant que vous avez gagné à la loterie. Pour encaisser vos gains, vous devez appeler le numéro indiqué dans le message et fournir vos informations bancaires. Lorsque vous appelez le numéro de téléphone, une personne vous explique que vous devez payer des frais de transaction ou des taxes avant de recevoir vos gains de loterie. Une fois que vous leur fournissez ces informations financières et que vous payez les frais exigés, les cybercriminels disparaissent avec votre argent et vos informations, vous ne les reverrez jamais. La façon la plus simple de vous protéger contre ce type d'attaques est de se méfier de tout message qui vous semble trop beau pour être vrai. Dans ce cas, comment pourriez-vous gagner à une loterie à laquelle vous n'avez pas participé et dont vous n'avez jamais entendu parler auparavant ?

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse:
securite.informatique@lausanne.ch

Lausanne

Email

Le courriel est un moyen efficace pour communiquer, mais c'est aussi l'une des méthodes d'attaque les plus communément utilisées par les cybercriminels de nos jours. Faites preuve de bons sens. Si un email vous semble étrange, suspect ou trop beau pour être vrai, c'est certainement une attaque.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse:
securite.informatique@lausanne.ch

Lausanne

Email

L'email est devenu l'une des principales méthodes de communication. Non seulement nous l'utilisons tous les jours au travail, mais aussi pour rester en contact avec nos amis et notre famille. De plus, c'est l'outil qu'utilisent la plupart des organisations pour fournir leurs produits et leurs services, par exemple pour la confirmation d'un achat en ligne ou pour accéder à vos relevés de compte bancaire. Dans la mesure où tant de personnes dans le monde entier dépendent des emails, les attaques ciblant les emails (que l'on appelle généralement phishing ou hameçonnage) sont devenues l'un des principaux modes d'attaque des cybercriminels. Dans ce bulletin d'informations, nous vous expliquons ce qu'est le phishing et les mesures à suivre pour vous protéger.

Le phishing est un terme utilisé pour décrire, à l'origine, des attaques électroniques qui ont été conçues pour dérober votre nom d'utilisateur et votre mot de passe de services bancaires en ligne. Toutefois, le terme a évolué et se réfère maintenant à presque toute attaque par messagerie électronique. Le phishing utilise l'ingénierie sociale, une technique où les cybercriminels tentent de vous pousser à agir. Ces attaques commencent quand un cybercriminel vous envoie un email prétendant être une personne ou une entité que vous connaissez ou en qui vous avez confiance, comme un ami, votre banque ou votre commerçant préféré. Leur but est de vous inciter à faire une action, par exemple, cliquer sur un lien malveillant, ouvrir une pièce jointe infectée ou répondre à une escroquerie. Les cybercriminels élaborent ces e-mails pour qu'ils soient convaincants et les envoient à des millions de personnes dans le monde. Ces criminels n'ont pas une cible spécifique à l'esprit, ils ne savent pas exactement qui seront leurs victimes. Ils savent tout simplement que plus ils envoient d'e-mails, plus ils seront en mesure de tromper de nombreuses personnes.

Vous protéger

Dans la plupart des cas, le simple fait d'ouvrir un e-mail ne présente aucun risque. Pour que la plupart des attaques fonctionnent, vous devez faire quelque chose après avoir lu l'e-mail, comme par exemple ouvrir un fichier joint, cliquer sur un lien ou répondre en donnant des informations. Afin de vous protéger, gardez en tête les points suivants :

- Le simple fait qu'un e-mail provienne d'un ami ne signifie pas que le message est sûr. Les cybercriminels peuvent avoir infecté l'ordinateur de votre ami, piraté son compte ou falsifié l'adresse de provenance. Si vous avez des soupçons à propos d'un message reçu d'une connaissance, appelez cette personne pour vérifier que c'est bien elle qui vous a envoyé ce message.
- Restez sur vos gardes à chaque fois que vous recevez un e-mail commençant par « cher client » ou par une autre salutation générique.
- Restez sur vos gardes lorsque vous recevez des e-mails qui vous demandent d'accomplir des « actions immédiates », et qui créent ainsi un sentiment d'urgence, ou ceux qui vous menacent de fermer votre compte.
- Méfiez-vous des messages affirmant provenir d'organismes officiels, mais qui sont pleins de fautes de grammaire ou d'orthographe. La plupart des organismes font appel à des rédacteurs professionnels, qui ne font pas ces fautes.
- Avant de cliquer sur un lien, survolez-le avec votre souris. Cela permettra d'afficher la véritable adresse de destination de ce lien. Vérifiez que la destination affichée correspond à la destination mentionnée dans l'e-mail et vous dirige vers le site légitime de l'organisation. Le mieux serait encore de taper le nom du site dans votre navigateur. Par exemple, si vous recevez un e-mail de

votre banque vous demandant de mettre à jour votre compte bancaire, ne cliquez pas sur le lien. Recherchez plutôt le site de votre banque dans votre navigateur et identifiez-vous directement à partir de celui-ci. Vous utilisez un appareil portable ? Aucun problème. Maintenez simplement votre doigt sur le lien, et vous pourrez voir la véritable destination s'afficher dans une fenêtre pop-up.

- Faites attention aux pièces jointes et n'ouvrez que celles que vous attendez . La plupart des pièces jointes infectées, envoyées de nos jours, peuvent contourner votre anti-virus.
- N'oubliez pas que c'est vous, qui êtes souvent la plus grande source de risques. Vérifiez toujours que vous envoyez l'email à la bonne personne avant de l'envoyer, en particulier pour des informations sensibles. Par exemple, avec les fonctionnalités du courriel, comme l'auto-remplissage, vous pouvez essayer d'envoyer un email au service des finances, mais envoyer le mail à un vieil ami accidentellement.

En fin de compte, une utilisation sûre des e-mails et de la messagerie instantanée relève du bon sens. Si quelque chose vous semble suspect, ou trop beau pour être vrai, c'est sûrement le cas. Supprimez simplement le message. Si vous recevez un message et vous n'êtes pas sûr qu'il s'agisse d'une attaque, contactez votre assistance technique ou l'équipe de sécurité informatique.

Les escroqueries à l'hameçonnage

Jusqu'à présent, nous avons discuté de toutes les agressions qui sont conçues pour attaquer autant de personnes que possible. En plus de ces attaques généralisées, les cybercriminels utilisent des attaques plus ciblées appelées « escroqueries à l'hameçonnage. » C'est une attaque hautement personnalisée consistant à envoyer seulement quelques courriels à des individus spécifiques au sein de notre entreprise.

La raison pour laquelle ces attaques ciblées sont plus dangereuses, c'est que les criminels font des recherches approfondies au préalable. Ils commencent par analyser qui travaille dans notre entreprise, avant de cibler des employés spécifiques (comme vous) et de recueillir autant d'informations que possible sur des sites comme LinkedIn ou Facebook. Quand ils ont collecté autant d'informations que possible sur vous, ils créent des emails d'hameçonnage personnalisés basés sur ces informations pour vous pousser à cliquer sur une pièce jointe infectée ou un lien malveillant.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse: securite.informatique@lausanne.ch

Lausanne

Navigateurs

Votre navigateur est, à bien des égards, votre porte d'accès à Internet. C'est également la cible principale des cybercriminels. En protégeant votre navigateur, vous vous protégez contre la plupart des attaques d'aujourd'hui.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse:
securite.informatique@lausanne.ch

Lausanne

Navigateurs

Internet est un outil puissant pour nos activités quotidiennes. Vous l'utilisez pour chercher des informations, faire des achats dans des boutiques en ligne, regarder des films ou gérer vos finances. Dans presque tous les cas, le principal outil que vous utilisez est un navigateur Internet, comme Internet Explorer, Chrome ou Firefox. Votre navigateur est à bien des égards, votre porte d'accès à Internet.

Dans la mesure où tant de gens, partout dans le monde, utilisent et dépendent des navigateurs pour leurs activités quotidiennes sur Internet, votre navigateur est la cible principale des cybercriminels. Les cybercriminels ont donc développé des techniques d'attaque et conçu des sites malveillants afin de pirater votre navigateur. Après le piratage, les criminels gagnent rapidement un contrôle total de votre ordinateur et de toutes vos informations sans que vous le sachiez. En protégeant votre navigateur et en l'utilisant judicieusement, vous pouvez vous protéger contre ces menaces et utiliser Internet en toute sécurité, pour vos activités quotidiennes.

Solution

Vous devriez toujours respecter ces mesures pour protéger votre navigateur et vous-même :

Votre navigateur

Tout d'abord, utilisez les versions les plus récentes de votre navigateur. La société qui a développé votre navigateur ajoute constamment de nouvelles mesures de sécurité et de nouvelles fonctionnalités pour améliorer sa protection. En utilisant la version la plus récente, vous êtes certain que vous disposez des derniers mécanismes de sécurité en place. Pour vous assurer que votre navigateur est toujours à jour, autorisez la mise à jour automatique. La mise à jour automatique permet à votre navigateur de vérifier continuellement l'existence de nouveaux correctifs. Dès qu'un nouveau correctif est sorti, votre navigateur ou votre système d'exploitation va télécharger ces correctifs et mettre à jour le navigateur.

Évitez les plugins

Les plugins ou les add-ons sont des programmes supplémentaires que vous pouvez installer dans votre navigateur pour vous donner plus de fonctionnalités. Par exemple, Adobe Flash, Java et QuickTime d'Apple. Chaque plugin que vous ajoutez devient un point d'accès supplémentaire qui permet aux agresseurs de pénètrer dans votre ordinateur. En outre, il peut être difficile de conserver ces plugins à jour parce que très peu d'entre eux ont des fonctionnalités de mise à jour automatique. Installez uniquement les plugins autorisés et ceux dont vous avez absolument besoin, et assurez-vous toujours que vous avez installé la version la plus récente. Si vous n'utilisez plus un plugin, supprimez-le de votre navigateur.

Scannez tous les téléchargements

Scannez tous les fichiers téléchargés sur Internet à l'aide d'un antivirus. Lorsque vous téléchargez et installez ou lancez un nouveau programme, il se peut que ce programme soit infecté. Il peut vous sembler qu'il fonctionne correctement, mais en réalité, il tente d'infecter discrètement votre ordinateur. Cela est très

courant surtout avec les fichiers gratuits comme les écrans de veille, les lecteurs vidéo ou les jeux. Assurez-vous de scanner tout ce que vous téléchargez avec un antivirus.

Filtrage et protection sur Internet

Le filtrage du navigateur Internet (parfois appelé filtrage Smartscreen, listes noires ou protection anti hameçonnage) est une fonction prise en charge par la plupart des navigateurs. Cela vous empêche de visiter les sites Internet connus comme étant malveillants. Vous ne le savez peut-être pas, mais il y a des organisations de sécurité qui scannent en permanence le web et qui recherchent les sites malveillants. Dès qu'elles repèrent un site malveillant, elles l'ajoutent à leur base de données. La plupart des navigateurs modernes ont accès à ces bases de données. Si vous essayez de visiter un de ces sites, le navigateur bloquera votre tentative et vous expliquera que vous essayez de visiter un site malveillant connu. Si votre navigateur vous met en garde contre la visite d'un site comme celui-ci, ne vous connectez pas à ce site. Au lieu de cela, fermez simplement la fenêtre du navigateur sur laquelle vous vous trouvez. N'oubliez pas que cette fonction vous protège uniquement des sites malveillants connus. Elle ne peut pas vous protéger ou vous mettre en garde contre des sites malveillants que personne ne connaît.

Évitez les mauvais quartiers

De bien des manières, Internet ressemble à une grande ville. Il y a tout ce dont vous avez besoin, des banques et des centres commerciaux, des événements sportifs et des films. Cependant, comme toute grande ville, Internet a des bons quartiers et des mauvais quartiers. Les bons quartiers sont constitués de sites Internet que vous connaissez et auxquels vous faites confiance. Les mauvais quartiers rassemblent des sites conçus pour vous attaquer ou vous nuire, à vous ou à votre ordinateur. Ils piratent votre navigateur ou distribuent des logiciels infectés, par exemple de faux économiseurs d'écran ou des jeux infectés. Tout comme dans une grande ville, l'un des moyens les plus simples pour assurer sa sécurité est d'éviter les mauvais quartiers. Si vous n'avez jamais entendu parler d'un site Internet, si les informations de l'URL semblent incorrectes ou suspectes, ou si le site Internet semble donner des informations douteuses, ne téléchargez aucun logiciel et ne soumettez aucune information à ce site.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse: securite.informatique@lausanne.ch

Lausanne

Naviguer en toute sécurité sur les réseaux sociaux

Les réseaux sociaux sont des outils très puissants pour communiquer avec vos amis et votre famille dans le monde entier. Cependant, faites attention à ce que vous partagez, comment vous le partagez, et avec qui.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse: securite.informatique@lausanne.ch

Lausanne

Naviguer en toute sécurité sur les réseaux sociaux

Les réseaux sociaux représentent l'une des technologies les plus passionnantes d'Internet. Ce qui rend ces sites si puissants est qu'il est très facile de partager avec les autres nos activités, et de prendre connaissance de celles des autres. Cependant, toutes ces nouvelles possibilités génèrent de nouveaux risques que vous devriez connaître. Voici quelques mesures simples que vous pouvez prendre pour vous protéger en ligne.

Partager vos informations

Les réseaux sociaux vous permettent de publier et de partager une quantité énorme d'informations. Non seulement vous pouvez y publier des données personnelles, mais aussi vos chansons et vos films préférés, des photos et des événements de votre vie. Le problème, c'est que le partage de ces informations peut vous nuire si vous ne faites pas attention.

Les criminels et les agresseurs recherchent, par-dessus tout, les données très personnelles. Ils peuvent utiliser ces informations pour deviner vos mots de passe, pour se faire passer pour vous en ligne, ou même usurper votre identité en se fondant sur les informations personnelles que vous avez partagées. Ne publiez jamais d'informations personnelles telles que votre date de naissance, votre adresse privée ou vos numéros d'identification en ligne. En outre, les entreprises qui embauchent de nouveaux employés ou les universités qui recrutent de nouveaux étudiants effectuent des contrôles sur les sites populaires de réseautage social tels que Facebook. Pour protéger votre avenir, ne publiez aucune information ou photo gênante vous concernant. Si vous ne tenez pas à ce que votre patron ou des membres de votre famille voient ce que vous postez, alors ne le faites pas, tout simplement.

Vous devez aussi faire attention à ce que les autres postent sur vous. Des amis peuvent poster des informations confidentielles ou des photos personnelles de vous. Demandez à vos amis de prendre en compte votre confidentialité et suivez ce qu'ils postent à propos de vous. S'ils postent un contenu que vous estimez inapproprié, demandez-leur de retirer ce contenu ou signalez-le au service des abus de ce site.

Faire confiance aux autres

Les criminels peuvent tenter de vous abuser sur des sites de réseaux sociaux, comme pour les emails ou les messageries. Une autre attaque commune sur Facebook et Twitter se produit lorsque les criminels piratent le compte d'une personne et postent des messages en se faisant passer pour cette dernière.

Par exemple, un ami peut poster un message indiquant qu'il s'est fait agresser à l'étranger, et qu'il a perdu son argent et ses documents. Il a désespérément besoin d'aide et demande si vous ou quelqun d'autre, pourriez faire un virement immédiat. Mais en fait, votre ami ne s'est jamais fait agresser. Il n'était même pas en voyage. C'est un criminel qui a piraté le compte Facebook de votre ami et qui a posté de faux messages en son nom. Comme pour les emails, si vous recevez des messages suspects d'un site de réseaux sociaux de la part d'un ami, appelez cet ami pour vérifier s'il a bien posté ce message.

Naviguer en toute sécurité sur les réseaux sociaux

Applications et jeux tiers

Certains réseaux sociaux ont des programmes tiers tels que des jeux, que vous pouvez installer. Ces programmes ne sont habituellement pas développés ou examinés par le site de réseautage social ; ils sont élaborés indépendamment par d'autres individus ou entreprises. Soyez toujours prudent lors de l'utilisation de programmes tiers car ils peuvent potentiellement infecter votre ordinateur ou accéder à vos informations privées.

Informations professionnelles

Ne postez aucune information confidentielle à propos de notre organisation sur un site, quel qu'il soit. Si vous avez des questions sur ce que vous pouvez poster ou non à propos de votre travail, posez la question à votre supérieur. De plus, assurez-vous de ne pas utiliser vos mots de passe professionnels pour vos comptes de réseaux sociaux ; ces comptes personnels doivent avoir des mots de passe différents. De cette manière, si l'un des comptes de réseaux sociaux que vous utilisez, est piraté, vos mots de passe professionnels seront toujours en sécurité.

Vos paramètres de sécurité

La plupart des réseaux sociaux comme Facebook proposent des paramètres de confidentialité. Il s'agit de paramètres que vous pouvez configurer pour déterminer qui peut et qui ne peut pas accéder aux informations sur votre page. Le problème de ces paramètres, c'est qu'ils sont assez complexes; il est donc très facile de faire des erreurs. Vous pensez peut-être que vos renseignements sont protégés, mais vous serez peut-être surpris d'apprendre que d'autres peuvent y accéder. Et une fois que vous avez compris le fonctionnement des paramètres de confidentialité, il arrive assez souvent qu'ils soient modifiés. Finalement, si le compte de l'un de vos amis est piraté, vos informations peuvent être accessibles à l'agresseur. Le meilleur moyen de se protéger est de s'attendre à ce que n'importe quelle information que vous postez soit un jour rendue publique, quels que soient vos paramètres de confidentialité. Si vous ne tenez pas à ce que votre patron, vos collègues ou des membres de votre famille voient ce que vous postez, alors ne le faites pas, tout simplement.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse: securite.informatique@lausanne.ch

Lausanne

Sécurité des appareils portables

Les appareils portables tels que les smartphones et les tablettes sont devenus l'une des principales méthodes pour communiquer et de bien des manières, ils remplacent les ordinateurs. Suivez donc ces mesures pour vous protéger.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse:
securite.informatique@lausanne.ch

Lausanne

Sécurité des appareils portables

Les appareils portables, tels que les smartphones ou les tablettes, sont devenus incroyablement puissants. Vous pouvez non seulement appeler le monde entier avec, mais vous pouvez aussi, à présent, regarder des films, lire vos e-mails, consulter votre banque en ligne et même installer des applications. Tous ces facteurs rendent les appareils portables très utiles. Toutefois, ils peuvent également représenter un très gros risque. Afin de vous protéger, gardez en tête les points suivants :

- Tout comme pour votre ordinateur, n'installez que les applications dont vous avez vraiment besoin et assurez-vous de les télécharger à partir de sources sûres. Les criminels peuvent créer des applications aux apparences réelles, mais qui sont en fait des programmes mal intentionnés conçus pour prendre discrètement le contrôle de vos appareils. En outre, n'installez pas d'applications qui demandent des autorisations excessives, comme la possibilité d'envoyer des messages texte silencieusement ou de copier votre carnet d'adresses.

- Tout comme pour votre ordinateur, faites des sauvegardes régulières sur vos appareils portables. De cette façon, si quelque chose arrivait à vos appareils, vos informations ne seraient pas perdues.

- Tout comme pour votre ordinateur, faites des sauvegardes régulières sur vos appareils portables. Les cybercriminels peuvent exploiter plus facilement vos appareils si vous utilisez des programmes trop anciens. Si votre appareil portables est vieux et n'est plus pris en charge, envisagez d'en acheter un nouveau qui peut prendre en charge la dernière version du système d'exploitation et des mises à jour de sécurité.

- Ne faites jamais de jailbreaking ou ne piratez jamais votre propre appareil portable. Non seulement votre appareil peut ne plus être pris en charge, mais généralement, cela paralyse ou désactive beaucoup des dispositifs de sécurité conçues pour protéger vos informations et vous-même.

- Si vous avez installé des programmes de sécurité tels que des antivirus ou des pare-feux, assurez-vous de les avoir activés et correctement mis à jour avec les dernières versions.

- N'oubliez pas que bon nombre des attaques que vous trouvez dans vos e-mails peuvent aussi se répandre par les SMS sur vos appareils portables. Par exemple, les cybercriminels peuvent envoyer des messages vous demandant de vous connecter sur des sites malveillants, de télécharger des applications infectées, ou vous demandant des informations privées telles que vos coordonnées bancaires. Si un message texte vous semble étrange ou trop beau pour être vrai, supprimez-le tout simplement.

- Soyez prudent lorsque vous utilisez le Wi-Fi. Beaucoup d'appareils portables se connectent automatiquement sur des réseaux Wi-Fi sans vous le demander, et exposent vos appareils à des risques. Désactivez le Wi-Fi si vous ne l'utilisez pas.

Sécurité des appareils portables

- Les criminels peuvent aussi tirer parti des capacités de votre Bluetooth. Tout comme pour le Wi-Fi, désactivez le Bluetooth lorsque vous ne l'utilisez pas. Il est aussi important de désactiver la fonction d'identification par Bluetooth.

- N'accédez pas ou ne stockez pas d'emails professionnels ou de données de notre organisation sur votre appareil portable, sauf si vous avez reçu l'autorisation à ces fins et si les protections de sécurité sont en place.

Enfin, si vous perdez un de ces appareils, n'importe qui peut lire vos informations, y compris vos emails, vos photos ou vos listes de contact, sauf si ces éléments sont protégés. Pour protéger vos appareils, veillez à les verrouiller avec un code ou mot de passe difficile à deviner. Si votre appareil propose le chiffrement, nous vous recommandons de l'utiliser. Pensez également à activer le nettoyage à distance si cette option est disponible. Cela signifit que si votre appareil portable est perdu ou volé, vous pouvez effacer toutes les informations à distance. Si vous perdez ou vous faites voler l'appareil mobile que vous a donné notre organisation ou un appareil contenant des informations sur l'organisation, vous devez avertir le service d'assistance ou l'équipe en charge de la sécurité des informations immédiatement.

Éliminer vos appareils

De nouveaux appareils portables munis de fonctionnalités indispensables sortent tous les mois. En conséquence, nombreux sont ceux qui remplacent leur smartphone ou leur tablette presque tous les ans. Mais qu'advient-il de votre vieil appareil quand vous devez vous en débarrasser ? Plus important encore : que vont devenir toutes vos informations confidentielles ? Après avoir utilisé vos appareils tous les jours pendant si longtemps, ils ont accumulé une quantité incroyable de données très privées. Avant de vendre ou de vous débarrasser de tout appareil portable, veiller à effacer toutes les informations qu'il peut contenir. Assurez-vous de retirer la carte SIM ou toute carte Flash de l'appareil avant de vous en débarrasser. Si votre appareil portable vous a été donné par notre organisation, assurez-vous de contacter le service d'assistance ou l'équipe en charge de la sécurité des informations qui vous diront comment vous en débarrasser.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse: securite.informatique@lausanne.ch

Lausanne

Mots de passe

Vos mots de passe sont les clés de votre royaume, protégez-les donc judicieusement. Dans ce bulletin d'informations, nous allons vous montrer comment créer des mots de passe solides que les cyber-criminels auront du mal à deviner et nous vous indiquerons comment les utiliser en toute sécurité.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse:
securite.informatique@lausanne.ch

Lausanne

Mots de passe

Si quelqu'un peut avoir accès à vos mots de passe, il peut voler votre identité électronique et avoir accès à toutes vos informations. Découvrons ensemble les éléments constituant de bons mots de passe et comment les utiliser en toute sécurité. Il y a deux points clés à retenir pour élaborer de bons mots de passe :

- Tout d'abord, il faut que vos mots de passe soient difficiles à deviner. En d'autres termes, il ne faut pas utiliser de mots de passe comme 123456, les noms de vos animaux domestiques ou encore votre date de naissance.
- Ensuite, utilisez des mots de passe faciles à retenir. Si vous les oubliez continuellement, ils ne vous seront pas d'une grande aide.

Le problème, c'est que les cybercriminels ont développé des programmes qui automatisent la capacité à deviner, ou qui forcent vos mots de passe, et ils s'améliorent en permanence. Cela veut dire qu'ils peuvent alors s'introduire dans vos comptes si vos mots de passe sont faciles à deviner. Afin de vous protéger, votre mot de passe doit être aussi long que possible. Plus votre mot de passe est long, plus il est fort. En fait, au lieu d'utiliser un seul mot comme mot de passe, utilisez plusieurs mots, on parle alors de phrase-mot de passe. Par exemple, cela pourrait être :

Où est mon café ?

Pour que votre phrase-mot de passe soit encore plus sécurisée, pensez par exemple à :

- Utiliser un chiffre dans votre phrase-mot de passe.
- Utiliser au moins une lettre en minuscule et une lettre en majuscule dans votre phrase-mot de passe.
- Utiliser un symbole dans votre phrase-mot de passe.

Par exemple, vous pouvez remplacer la lettre « o » par le chiffre zéro ou la lettre « e » par le chiffre trois. En outre, vous utilisez des symboles lorsque vous utilisez des signes de ponctuation courants tels que les espaces, un point d'interrogation ou un point d'exclamation. Par conséquent, vous pouvez avoir un mot de passe fort, qui est très difficile à deviner pour les cybercriminels, mais qui est simple à retenir et facile à taper. En plus d'avoir des mots de passe forts, vous devez protéger la façon dont vous les utilisez :

- Assurez-vous d'utiliser des mots de passe différents pour des comptes différents. Par exemple, n'utilisez jamais le même mot de passe pour un compte professionnel ou bancaire et un compte personnel comme Facebook, YouTube ou Twitter. Ainsi, si l'un de vos mots de passe est piraté, les autres comptes restent sécurisés. Ne communiquez jamais vos mots de passe à quiconque. Cela est valable pour vos collègues. N'oubliez pas, si votre mot de passe est un secret, il n'est plus sécurisé dès que quelqu'un d'autre le connaît.

- N'utilisez jamais votre mot de passe sur un ordinateur public, comme les ordinateurs présents dans un hôtel ou une bibliothèque, pour vous connecter à un compte professionnel ou bancaire. Dans la mesure où tout le monde utilise ces ordinateurs, ils peuvent facilement être infectés par un code malicieux qui enregistre vos saisies sur le clavier. Connectez-vous à vos comptes professionnels ou bancaires uniquement en utilisant des ordinateurs fiables ou des appareils portables que vous contrôlez.

Mots de passe

- Si vous partagez accidentellement votre mot de passe avec quelqu'un, ou si vous pensez que votre mot de passe peut avoir été compromis ou dérobé, assurez-vous de le changer immédiatement.

- Méfiez-vous des sites vous posant des questions personnelles. Ces questions sont utilisées si vous oubliez votre mot de passe et servent à le réinitialiser. Le problème, c'est que les réponses à ces questions se trouvent souvent sur Internet ou sur votre page Facebook. Assurez-vous d'utiliser uniquement des informations qui ne sont pas connues publiquement, si vous répondez à des questions personnelles.

- De nombreux comptes en ligne proposent ce que l'on appelle l'authentification à deux facteurs. Dans ce cas, vous avez besoin d'un autre élément que votre mot de passe pour vous connecter, par exemple un code envoyé sur votre smartphone. Dès que possible, utilisez toujours ces méthodes d'authentification plus sécurisées.

- Enfin, lorsque vous n'utilisez plus un compte, assurez-vous de le désactiver ou de le supprimer.

Gestionnaires de mots de passe

Un des points clés que nous avons abordés dans ce bulletin insiste sur la nécessité d'avoir un mot de passe unique pour chacun de vos comptes. De cette façon, si un compte est compromis, vos autres comptes restent sécurisés. Cependant, vous pouvez avoir tellement de comptes que vous ne pouvez pas retenir tous les différents mots de passe. Si c'est le cas, envisagez d'utiliser un gestionnaire de mots de passe. C'est un programme spécial que vous lancez sur votre ordinateur qui stocke en toute sécurité tous vos mots de passe. Les seuls mots de passe que vous devez retenir sont ceux de votre ordinateur et de votre programme de gestion de mots de passe. Certains gestionnaires de mots de passe sont même intégrés à votre navigateur, assurant la connexion aux différents sites Internet pour vous. Vérifiez avec votre superviseur, le service d'assistance ou l'équipe de sécurité des informations pour savoir si vous pouvez utiliser un gestionnaire de mots de passe.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse: securite.informatique@lausanne.ch

Lausanne

Chiffrement

Votre ordinateur portable, vos appareils portables et vos lecteurs flash USB stockent une quantité énorme de données sensibles. Toutefois, si vous perdez un de ces appareils, n'importe qui peut lire vos informations, y compris vos emails, vos documents et vos photos. En chiffrant vos données, vous empêchez aux personnes non autorisées d'y accéder.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse:
securite.informatique@lausanne.ch

Lausanne

Chiffrement

La quantité d'informations que vous transportez aujourd'hui est tout simplement impressionnante. L'un des moyens les plus courants pour mesurer l'information est le giga-octet. Un seul gigaoctet peut stocker plus de 7000 documents Word, ou 2000 images. A titre de comparaison, une clé USB ou un smartphone peut stocker plus de 128 giga-octets. Un nouveau portable peut stocker des milliers de giga-octets (on parle alors de téraoctets) de données. Chacun de ces appareils est facile à transporter avec vous et cela vous permet de quitter le bureau avec une quantité énorme d'informations confidentielles, telles que notre base de données sur les clients, des courriers électroniques sensibles ou des milliers de documents de travail. Malheureusement, il est également facile de perdre un de ces appareils. Une fois que l'un de ces appareils est perdu, toutes vos informations et toutes les informations sensible de notre organisation peuvent potentiellement être compromises.

Solution

Mais quelle est donc la solution ? Une méthode pourrait consister à ne jamais quitter le bureau avec des informations sensibles. Selon votre poste, cela peut être votre cas. Cependant si votre supérieur vous a donné la permission de vous déplacer avec des informations sensibles, vous avez besoin d'un moyen pour protéger ces données. Cette méthode, c'est le chiffrement.

Le chiffrement est le processus consistant à transformer des informations normales (appelée données non chiffrées ou en clair) et à les rendre illisibles (texte chiffré ou crypté). Le chiffrement utilise des formules mathématiques, appelées « algorithmes », et une clé unique pour convertir les données dans un format non lisible par l'utilisateur appelé « texte chiffré ». La clé est ce qui verrouille ou déverrouille votre information, tout comme une clé peut verrouiller ou déverrouiller une porte. Le mot de passe est un exemple commun de clé de chiffrement, celui qui a la clé peut déchiffrer et déverrouiller vos informations. Pour protéger vos données chiffrées, vous avez tout d'abord besoin de protéger votre clé. Par exemple, si votre ordinateur portable est chiffré et que vous le perdez pendant un déplacement, les données de votre ordinateur portable sont en sécurité tant que personne ne connaît le mot de passe. La seule manière d'accéder à votre ordinateur portable, c'est de connaître le mot de passe pour déchiffrer les données.

Auparavant, le chiffrement était difficile à mettre en œuvre. Il fallait identifier quelles informations vous vouliez chiffrer sur votre ordinateur et configurer des programmes complexes pour chiffrer les informations. Il fallait ensuite déchiffrer manuellement les données chaque fois que vous en aviez besoin. Cette approche était difficile et prennait beaucoup de temps. Aujourd'hui, les solutions sont beaucoup plus simples. En général, la meilleure approche est tout simplement de chiffrer tout votre système, ce qui est souvent appelé chiffrement intégral du disque. Cela signifie que vous n'avez pas à vous soucier des données à chiffrer ou

comment les chiffrer car absolument tout sur votre appareil est chiffré. Ainsi, quand vous ouvrez une session ou vous accédez à votre appareil, tout est déchiffré automatiquement.

En outre, le chiffrement peut non seulement aider à protéger les informations sur vos appareils, mais peut aussi aider à protéger vos informations, quand elles sont transférées sur le réseau. Par exemple, lorsque vous utilisez votre navigateur pour vous connecter à votre banque en ligne, cette connexion doit être chiffrée pour protéger toutes vos informations financières sensibles. Vous pouvez également recevoir un réseau privé virtuel (VPN) de notre organisation. C'est une couche supplémentaire de chiffrement qui protège toutes vos activités en ligne.

Pour en savoir plus sur les programmes de chiffrement proposés qui chiffrent automatiquement vos informations, veuillez contacter le service d'assistance ou l'équipe de sécurité des informations.

Chiffrer les appareils personnels

Le chiffrement n'est pas seulement réservé au travail. Nous vous recommandons fortement d'envisager de l'utiliser pour votre vie personnelle également. Vous transportez sur vous une énorme quantité de renseignements très personnels, des photos de famille sur votre smartphone aux e-mails personnels sur votre ordinateur portable. Tout comme pour le travail, si l'un de ces appareils est perdu ou volé, tout le monde peut accéder à vos informations. Heureusement, la plupart des appareils proposent le chiffrement de nos jours.

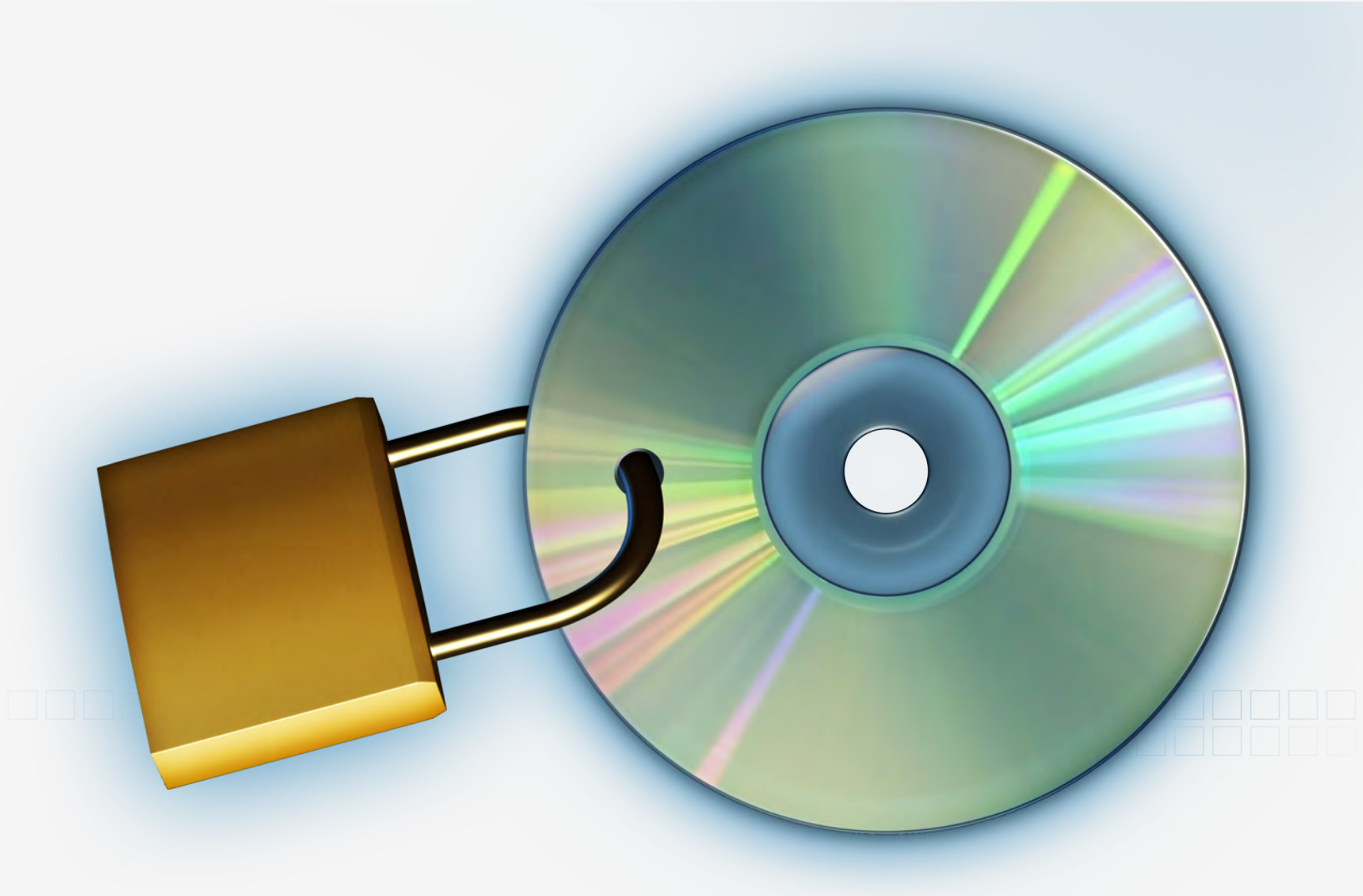
Pour les utilisateurs de Windows, selon la version de Windows que vous avez, votre ordinateur peut être livré avec une technologie de chiffrement gratuite que vous pouvez utiliser, nommée Bitlocker. Pour les utilisateurs de Mac OS X, vous pouvez chiffrer vos ordinateurs portables en utilisant la technologie gratuite nommée FileVault. Beaucoup d'appareils portables prennent également en charge le chiffrement. Cependant, le chiffrement est généralement activé uniquement si vous installez un code PIN ou un mot de passe. Assurez-vous de toujours protéger vos appareils portables par un mot de passe.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse: securite.informatique@lausanne.ch

Lausanne

Sécurité des données

Nos informations sont notre plus grand bien ; elles sont également la cible principale de nombreux cybercriminels. La technologie seule ne suffit pas à protéger nos données extrêmement précieuses. Il est essentiel que vous adoptiez ces mesures pour participer à la protection de nos informations sensibles.



Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse: securite.informatique@lausanne.ch

Lausanne

Sécurité des données

Nous concentrons une grande partie de nos efforts sur l'entretien de la sécurité de nos appareils, avec par exemple l'utilisation de pare-feux, d'antivirus et des mises à jour régulières. Il est important de comprendre que la plupart des criminels ne veulent pas seulement prendre le contrôle de votre ordinateur ou de vos appareils portables. Ce sont plutôt les informations qu'ils contiennent qui les intéressent. Les informations sensibles peuvent être, par exemple, des choses secrètes de notre organisation, des relevés bancaires, des détails médicaux, des numéros de carte de paiement ou des informations personnelles identifiables. C'est pourquoi il faut vous assurer de bien prendre les mesures suivantes, lorsque vous gérez des informations sensibles :

- Comprenez toujours le niveau de sensibilité des données avec lesquelles vous travaillez. Si vous n'êtes pas sûr du niveau de sensibilité des informations ou des mesures que vous devriez suivre pour les sécuriser, demandez à votre superviseur.
- Utilisez uniquement les systèmes autorisés par notre entreprise pour saisir, traiter ou stocker des informations sensibles. Ne copiez ou ne stockez jamais d'informations sensibles sur des systèmes ou comptes non autorisés tels que des ordinateurs portables personnels ou des comptes de courriel personnels.
- Si vous avez l'autorisation de bénéficier d'un accès privilégié à un système, connectez-vous toujours avec votre identifiant unique non privilégié, puis élevez vos privilèges uniquement lorsque cela est nécessaire. Ne vous connectez jamais directement en tant qu'utilisateur privilégié.
- Si vous transférez des informations sensibles, utilisez des moyens autorisés proposant le chiffrement. Ne transférez jamais de données sensibles à l'aide de moyens non sécurisés tel que l'email, sauf si vous utilisez un logiciel de chiffrement spécialisé pour lequel vous avez été correctement formé.
- Vous devez disposer d'une autorisation préalable pour stocker des informations sensibles sur un support amovible ou des systèmes de stockage portables, comme les CD, DVD, clés USB et disques durs externes. Si vous avez reçu l'autorisation au préalable, toutes les informations doivent être chiffrées à l'aide d'un logiciel de chiffrement approuvé.
- N'enregistrez et ne partagez jamais d'informations sensibles au moyen de services publics d'Internet ou de services Cloud comme Dropbox, Apple iCloud ou encore Google Drive, à moins d'avoir reçu une autorisation préalable de votre direction.
- Faites attention lorsque vous répondez aux e-mails ou à des appels téléphoniques, dans lesquels il vous est demandé d'envoyer des informations sensibles. Veillez à toujours identifier au préalable la personne à l'aide de méthodes approuvées et veuillez vous assurer que cette personne est autorisée à accéder à ces informations avant de partager quoi que ce soit avec elle.
- Ne laissez jamais de documents sensibles sur votre bureau sans attention. Assurez toujours la sécurité des documents sensibles en les laissant, par exemple, enfermés dans une armoire sécurisée. En outre, à chaque fois que vous quittez votre ordinateur, assurez-vous qu'il est protégé à l'aide d'un mot de passe. De cette manière, vous serez certain que le personnel non autorisé ne pourra pas accéder à vos informations confidentielles en votre absence.

Sécurité des données

- Utilisez uniquement les logiciel autorisés pour les activités professionnelles. N'installez jamais ou n'utilisez jamais de logiciels sans licence, ni autorisation.
- Tout fournisseur tiers recevant des informations sensibles, ou y ayant accès, doit préserver ces données. Cela peut nécessiter un contrat, ou une évaluation des méthodes de contrôle de sécurité de ce fournisseur, pour s'assurer de la protection adéquate des données.
- Toute donnée sensible qu'il n'est plus nécessaire ou approprié de stocker doit être détruite, déchiquetée ou rendue illisible de manière appropriée par une méthode conforme à nos pratiques de conservation des archives.
- Si vous croyez que des données sensibles ont été perdues, volées ou compromises, n'oubliez pas de contacter l'assistance technique ou le service en charge de la sécurité informatique immédiatement. Plus tôt notre entreprise est avertie, plus tôt nous pouvons agir pour minimiser les dommages causés par un tel incident.

Ces mesures doivent être appliquées d'une manière conforme à nos politiques. Il est essentiel pour la sécurité de nos informations sensibles et de notre organisation que vous compreniez et suiviez nos politiques sur la sécurité des données.

Menaces avancées ciblant nos données

Il existe de nombreuses menaces ciblant nos données sensibles. Les cybercriminels sont la plus fréquente de ces menaces. Il s'agit d'individus ou d'entreprises qui volent nos données sensibles et les utilisent pour commettre des fraudes, ou tout simplement, qui les vendent à d'autres cybercriminels. Malheureusement, il y a de nombreuses autres menaces ciblant nos données sensibles, certaines de ces menaces étant bien plus sophistiquées que les cybercriminels communs.

Parmi ces menaces, il y a la concurrence. Certains de nos concurrents peuvent avoir des comportements très peu éthiques. Ils peuvent essayer de compromettre notre entreprise pour remporter un avantage concurrentiel ; pour cela ils ont besoin de nos données. D'autres menaces peuvent provenir de pays, qui peuvent cibler nos données à des fins économiques, politiques ou militaires. Ces pays disposent de hackers très compétents dont le travail à plein temps peut consister à pirater notre entreprise. Peut-être pensez-vous que vos données n'ont aucune valeur, mais détrompez-vous, elles sont très précieuses.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse: securite.informatique@lausanne.ch

Lausanne

Sécurité Wi-Fi

La technologie sans fil (souvent appelée Wi-Fi) vous permet de vous connecter simplement à Internet. Cependant, cette technologie simplifie aussi la tâche des cybercriminels, qui peuvent surveiller et voler vos informations. Dans ce bulletin d'information, nous couvrirons les mesures les plus efficaces pour vous aider à vous protéger quand vous utilisez le réseau sans fil.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse:
securite.informatique@lausanne.ch

Lausanne

Sécurité Wi-Fi

Aux débuts de l'Internet, la seule façon de se connecter était de passer par un réseau physique. Vous deviez physiquement brancher un câble réseau sur votre ordinateur ou sur votre ordinateur portable. Même s'ils n'étaient pas très pratiques pour l'utilisateur, les câbles physiques aidaient à protéger notre entreprise. Ils nous permettaient de contrôler qui avait accès à nos réseaux. Toutefois, le monde a eu besoin d'innover en créant un moyen plus rapide et plus simple de se connecter à des réseaux, un moyen qui ne nécessitait pas de câble. Par conséquent, une nouvelle technologie sans fil a émergé dans les années 1990, cette technologie se nomme le Wi-Fi. Le Wi-Fi permet à un ordinateur de se connecter à n'importe quel réseau sans câble.

Avec le Wi-Fi, vous sélectionnez simplement un réseau sans fil depuis votre ordinateur et vous vous y connectez. Dans certains cas, il vous est demandé de fournir un identifiant et un mot de passe. Malheureusement, les réseaux Wi-Fi comportent certains risques que vous devez connaître.

Surveillance

Tout ce que vous faites sur un réseau sans fil peut être surveillé. Le réseau sans fil est similaire à une conversation, toute personne assez proche de vous peut écouter ce que vous dites et connaître vos activités. En plus de surveiller vos conversations, les criminels peuvent parfois utiliser votre connexion non sécurisée pour compromettre votre ordinateur ou vos comptes en ligne. Par conséquent, à chaque fois que vous vous connectez avec un réseau Wi-Fi, nous vous recommandons de le faire de manière sûre et de chiffrer toutes vos activités en ligne. Ceci est surtout important pour les réseaux publics, car nous ne pouvons pas garantir leur sécurité. En outre, vérifiez si vous pouvez utiliser un VPN (Virtual Private Network) pour vous connecter à distance depuis des points Wi-Fi publics. Cela permet de créer un canal chiffré, et vous pouvez ainsi travailler en ligne de manière plus sécurisée.

Se connecter à un réseau Wi-Fi

Pour vous connecter à un réseau sans fil, vous devez tout d'abord sélectionner le réseau auquel vous souhaitez vous connecter. Dans les endroits bondés ou publics, il y a souvent plusieurs réseaux au choix. Cependant, soyez toujours prudent lorsque vous vous connectez à des réseaux. Les cybercriminels peuvent créer de faux réseaux sans fil conçus pour nuire ou surveiller tout ce que vous faites. Pour vous protéger, assurez-vous toujours de vous connecter à un réseau Wi-Fi digne de confiance.

Lorsque vous êtes au travail, votre administrateur de réseau vous dira quel réseau sans fil vous pouvez rejoindre. Ces réseaux nécessitent presque toujours un identifiant de connexion et un mot de passe. Vous pouvez faire confiance à ces réseaux, car ils sont administrés par notre entreprise. Lorsque vous souhaitez vous connecter aux réseaux Wi-Fi dans les lieux publics (par exemple dans des hôtels ou des aéroports),

recherchez les panneaux vous indiquant les réseaux sans fil légitimes et comment y accéder. En vous assurant que vous vous connectez uniquement aux réseaux sans fil fiables, vous vous protégez contre tous les types d'attaques.

Enfin, quand vous vous connectez à des réseaux publics, partez du principe que ces réseaux sont hostiles. Toute personne se connectant à ce réseau peut scanner, examiner ou pirater un autre appareil connecté à ce réseau. C'est pour cela qu'il est si important que votre ordinateur portable et vos appareils portables soient sécurisés. Assurez-vous de bien utiliser la version la plus récente et de disposer des patchs et des logiciels les plus récents. En outre, assurez-vous que votre pare-feu est activé et que votre anti-virus tourne sur votre ordinateur portable.

Nos installations

Enfin, vous devez disposer d'une autorisation préalable pour installer des réseaux Wi-Fi au travail. Cela permet de garantir que les réseaux Wi-Fi de nos installations sont conformes à nos normes de sécurité et sont protégés contre les cybercriminels.

Wardriving

Le wardriving est une technique que les criminels utilisent pour trouver et pirater les organisations dont les réseaux sans fil sont vulnérables ou ouverts. Leur but ultime est généralement de trouver un réseau sans fil qui n'a pas d'authentification et que n'importe qui peut rejoindre. S'ils trouvent un de ces réseaux, ils peuvent tout simplement garer leur voiture dans notre parking, et accéder à notre réseau interne à partir de là. Ils utilisent une méthode nommée wardriving pour trouver ces réseaux sans fil non sécurisés. Le wardriving consiste tout simplement à circuler en voiture avec un ordinateur portable ouvert, en essayant de se connecter à des réseaux sans fil disponibles. Comme ces criminels sont au volant d'une voiture, ils peuvent couvrir une grande partie du territoire pour trouver rapidement et potentiellement des centaines de réseaux Wi-Fi vulnérables. C'est pourquoi nous prenons la sécurité très au sérieux et exigeons que tous les nouveaux réseaux Wi-Fi subissent des procédures de sécurité avant de pouvoir se connecter à l'un de nos réseaux.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse: securite.informatique@lausanne.ch

Lausanne

Travailler à distance

La technologie vous permet de plus en plus de travailler en dehors de votre lieu de travail, à la maison ou lorsque vous êtes en déplacement. Cela vous permet d'avoir une immense flexibilité, mais vous expose également à certains risques. Dans ce bulletin d'information, nous allons couvrir certaines mesures de base pour garantir votre sécurité.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse:
securite.informatique@lausanne.ch

Lausanne

Travailler à distance

La technologie vous permet de plus en plus de travailler en dehors de votre lieu de travail, à la maison ou lorsque vous êtes en déplacement. Cela vous permet d'avoir une immense flexibilité, mais vous expose également à certains risques. Nous allons vous montrer comment vous pouvez travailler efficacement et en toute sécurité lorsque vous n'êtes pas au bureau.

Travailler à la maison

Si vous avez la permission de travailler à domicile, n'oubliez pas que votre connexion et votre réseau à domicile ne sont sans doute pas aussi sécurisés que ceux de l'entreprise. En conséquence, certaines mesures supplémentaires doivent être prises pour vous protéger et pour protéger notre organisation.

Lorsque vous travaillez à domicile, utilisez uniquement les appareils autorisés à ces fins. N'utilisez pas d'appareils personnels, par exemple des ordinateurs personnels, sauf si vous avez reçu au préalable l'autorisation de votre direction. Dans ce cas, vous devrez peut-être installer un logiciel de sécurité complémentaire. Contactez le service d'assistance ou l'équipe en charge de la sécurité pour obtenir plus d'informations. Assurez-vous également que seules les personnes autorisées ont accès à tout système utilisé pour le travail. Enfants, invités ou autres membres du foyer ne doivent pas avoir accès à votre ordinateur de travail. Les utilisateurs non autorisés peuvent accidentellement infecter votre ordinateur ou endommager le système par d'autres moyens.

Se protéger des pertes

De plus, lorsque vous travaillez chez vous ou lorsque vous êtes en déplacement, assurez-vous que tous les appareils que vous utilisez professionnellement sont sécurisés sur le plan physique. Si vous devez par exemple laisser votre ordinateur portable dans votre voiture, enfermez-le dans le coffre à bagages. Si vous utilisez votre ordinateur portable pendant une conférence, pensez à utiliser un câble pour le sécuriser. En outre, effectuez toujours une double vérification et veillez à ne pas oublier vos appareils lors d'un voyage. Vous seriez surpris du nombre d'appareils perdus, tout simplement parce qu'on les a oubliés. Vérifiez toujours que vous n'avez pas oublié vos appareils lorsque vous passez au poste de sécurité de l'aéroport, lorsque vous quittez l'avion, lorsque vous rendez une voiture de location, ou lorsque vous quittez votre chambre d'hôtel.

Se connecter pour accéder aux activités professionnelles

Lorsque vous travaillez à distance, vous pouvez avoir besoin de vous connecter à nos réseaux internes. N'oubliez pas que lorsque vous le faites, vos activités et vos renseignements peuvent être contrôlés par d'autres. Lorsque vous vous connectez depuis le terminal d'un aéroport, un café ou un hall d'hôtel, ces réseaux publics sont accessibles par n'importe qui et ne doivent pas être considérés comme dignes de confiance. Toute connexion à distance incluant des informations professionnelles confidentielles doit être chiffrée. En outre, vous pouvez être amené à utiliser un logiciel VPN (Virtual Private Network) si vous devez vous connecter aux réseaux internes ou effectuer une activité professionnelle. Pour en savoir plus sur les exigences de chiffrement, veuillez contacter le service d'assistance ou votre équipe responsable de la sécurité.

Travailler à distance

Sécuriser vos appareils

Lors d'un déplacement, vous allez connecter votre ordinateur portable ou vos appareils portables à des réseaux publics non fiables. Vous ne savez jamais qui est connecté à ces réseaux. Vous devez vous assurer que vos appareils sont correctement sécurisés. Assurez-vous que les protections essentielles suivantes sont activées sur vos appareils :

- Assurez-vous que votre ordinateur portable et vos appareils portables disposent de la mise à jour automatique, ce qui vous permet de disposer des derniers correctifs et d'un système d'exploitation à jour.
- Assurez-vous que votre ordinateur portable et vos appareils portables disposent d'un mot de passe ou d'un code PIN pour protéger l'écran. Ainsi, personne ne peut y accéder si vous les perdez accidentellement.
- Assurez-vous qu'un anti-virus et un pare-feu sont installés et bien activés sur votre ordinateur portable.

Utiliser d'autres ordinateurs

Assurez-vous aussi de toujours utiliser des appareils agréés pour accéder à toute information concernant votre travail lors d'un déplacement. N'empruntez jamais un ordinateur public pour travailler, par exemple un ordinateur mis à disposition dans le hall d'entrée d'un hôtel, d'un aéroport, ou même l'ordinateur d'un ami. Ils pourraient être déjà infectés. En les utilisant, vous pourriez compromettre votre identifiant et votre mot de passe.

La perte de votre ordinateur portable

Il existe de nombreuses menaces dont vous devez tenir compte lorsque vous travaillez à distance. Vous devez vous préoccuper des cybercriminels qui peuvent essayer de pirater votre ordinateur ainsi que des criminels communs qui veulent voler votre ordinateur portable. Il y a une autre menace dont vous devez tenir compte: vous-même. La perte d'un smartphone ou d'un ordinateur portable est une source fréquente de compromission de données confidentielles. Dans bien des cas, il est plus probable que vous perdiez votre ordinateur portable plutôt qu'on ne vous le vole. Lorsque vous voyagez, il est très facile d'égarer ou d'oublier votre appareil portable ou votre ordinateur. Voici quelques conseils à ne pas oublier lors d'un déplacement.

- Rangez toujours votre ordinateur portable et votre smartphone dans le même sac ou le même endroit, il vous sera plus facile de voir s'ils n'y sont plus.
- Prenez l'habitude de vérifier si vous avez bien ces objets importants après avoir passer les points de sécurité, quand vous quittez un taxi ou quand vous quittez un avion.

Si vous avez perdu un objet lié à votre travail, signalez la perte immédiatement.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse: securite.informatique@lausanne.ch

Lausanne

Protection de votre ordinateur personnel

Tout comme votre ordinateur professionnel, votre ordinateur personnel est une cible constante. Cependant, votre ordinateur personnel ne bénéficie peut-être pas de toutes les mesures de sécurité que nous utilisons dans notre entreprise. Ce bulletin d'information vous présente quelques mesures à suivre pour vous protéger chez vous.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse:
securite.informatique@lausanne.ch

Lausanne

Protection de votre ordinateur personnel

Tout comme votre ordinateur professionnel, votre ordinateur personnel est une cible. Vos informations personnelles, vos comptes personnels, vos emails personnels, mais aussi votre ordinateur lui-même ont une valeur très élevée pour les cybercriminels. De plus, vous ne disposez pas d'une équipe de sécurité qui se consacre à le protéger au quotidien comme c'est le cas dans notre entreprise. Votre ordinateur personnel court donc des risques. Nous vous recommandons de suivre les simples mesures suivantes pour protéger vos ordinateurs personnels.

Solution

La première étape consiste à toujours vérifier que les derniers correctifs sont installés sur vos ordinateurs et que les programmes installés fonctionnent avec les dernières versions disponibles, par exemple pour votre navigateur. Les programmes trop vieux ou dépassés présentent de nombreuses faiblesses que les criminels peuvent exploiter. La manière la plus simple de vous protéger est d'activer l'option de mise à jour automatique pour votre ordinateur et vos programmes. Si vous n'utilisez plus un programme, supprimez-le ou désinstallez-le.

En plus de vous assurer de la mise à jour des programmes, vous devez vous assurer que les plugins de votre navigateur et les extensions sont à jour. Chaque plugin que vous ajoutez sur votre navigateur offre au cybercriminel un moyen supplémentaire pour vous pirater. Comme pour les programmes, si vous n'utilisez plus un plugin de navigateur, retirez-le ou désinstallez-le. Moins vous avez de plugins, moins votre navigateur présente de points de vulnérabilité. Nous vous recommandons de vérifier les plugins de votre navigateur au moins une fois par mois.

Afin de protéger votre vie privée en ligne, pensez à utiliser le mode privé de votre navigateur. Il s'agit d'un paramètre que la plupart des navigateurs proposent. Une fois activé, cela permettra de ne pas enregistrer votre activité en ligne (par exemple, les sites que vous visitez), de ne pas cacher les contenus des sites Internet, et habituellement de nettoyer tous les cookies enregistrés sur votre ordinateur. De nombreux navigateurs ont également une option de « réinitialisation » qui supprime toutes les informations stockées sur vos habitudes de navigation, par exemple les cookies stockés.

Il est très important de vous assurer qu'un pare-feu est bien installé et activé sur votre ordinateur. Les pare-feux protègent votre ordinateur des menaces telles que les scans de ports, les vers, et d'autres types de connexion malveillantes. De plus, assurez-vous d'utiliser un antivirus correctement mis à jour qui vous aidera à protéger votre système contre les chevaux de Troie, les virus et d'autres formes de programmes malveillants. Assurez-vous de configurer votre antivirus pour se mettre à jour automatiquement, car de nouvelles signatures sont émises en permanence. Si un antivirus ne peut pas détecter ou stopper tous les types de logiciels malveillants, il peut vous aider à vous protéger contre les versions les plus connues.

Protection de votre ordinateur personnel

Si votre ordinateur est un ordinateur portable, vous devrez peut-être prendre des mesures supplémentaires pour le protéger, surtout si vous voyagez avec. La première mesure consiste à toujours le sécuriser avec un identifiant de connexion et un mot de passe. Vous aurez très probablement besoin également d'un moyen de chiffrement, souvent nommé Full Disk Encryption. En combinant un mot de passe d'écran et le chiffrement, vous protégez votre ordinateur et ses informations en cas de perte ou de vol. En outre, vous pouvez installer un logiciel de suivi sur votre ordinateur portable. De cette façon, si vous le perdez (ou s'il est volé), vous pouvez suivre son emplacement ou effacer à distance toutes vos informations.

Enfin, faites des sauvegardes régulières de vos informations, par exemple vos photos de famille ou vos documents de valeur. Si votre ordinateur est piraté, la seule façon de le récupérer consiste souvent à réinstaller votre système d'exploitation et de récupérer vos dossiers personnels à partir d'une sauvegarde. N'oubliez pas, enfin, que vous êtes le meilleur système de protection de votre ordinateur et de vos appareils portables. Faites toujours preuve de bon sens. Si quelque chose vous semble suspect, ou trop beau pour être vrai, c'est sûrement une attaque.

Quel est le meilleur antivirus ?

Une question que nous recevons fréquemment est la suivante : quel est le meilleur logiciel antivirus, quel programme pare-feu devrais-je acheter ? Peu importe, tant qu'il s'agit d'un produit provenant d'une entreprise de sécurité digne de confiance. La plupart des produits à usage domestique ont des fonctions très similaires. Le produit le plus simple d'utilisation est probablement celui qui vous convient le mieux. La plupart des produits de sécurité sont de plus vendus en forfaits, cela signifie qu'il y a plusieurs programmes de sécurité, comme des pare-feux, des antivirus et des filtres Internet réunis dans une seule solution. L'avantage de ces forfaits, c'est que tous les outils dont vous avez besoin pour sécuriser votre ordinateur sont réunis dans un seul programme, une seule interface. Si vous achetez ce genre de solution, pensez à l'activer et à toujours disposer de la version la plus récente.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse: securite.informatique@lausanne.ch

Lausanne

Protection de votre réseau à domicile

Votre réseau à domicile, tout comme votre réseau au travail, est constamment attaqué. Voici quelques mesures que vous pouvez prendre pour vous protéger, vous et votre famille, à la maison.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse: securite.informatique@lausanne.ch

Lausanne

Protection de votre réseau à domicile

Les réseaux Wi-Fi (parfois appelés par leur nom technique, 802.11) permettent aux personnes de se connecter sans fil à l'Internet en utilisant des appareils comme des smartphones, des ordinateurs portables, des tablettes et des consoles de jeux. Dans la mesure où les réseaux Wi-Fi sont assez faciles à installer, beaucoup d'utilisateurs installent leurs propres réseaux à la maison. Cependant, de nombreux réseaux domestiques Wi-Fi sont configurés de manière non sécurisée, permettant à des étrangers ou à des personnes non autorisées d'accéder facilement à votre réseau domestique ou d'abuser anonymement de votre connexion Internet. Voici quelques mesures simples pour vous assurer de sécuriser votre réseau domestique Wi-Fi.

Solution

Votre réseau Wi-Fi est contrôlé par ce qu'on appelle un point d'accès Wi-Fi. Il s'agit d'un appareil physique que vous pouvez acheter dans votre magasin électronique local ou qui peut être intégré à votre routeur Internet. Le point d'accès est ce qui connecte vos appareils à Internet, par le réseau sans fil. Une des premières mesures pour sécuriser votre réseau Wi-Fi est de restreindre les personnes pouvant administrer votre point d'accès Wi-Fi et la manière dont elles peuvent y accéder. Nous vous recommandons de suivre les mesures suivantes lors de la configuration de votre point d'accès Wi-Fi pour la première fois.

1. Pour de nombreux points d'accès Wi-Fi, l'identifiant d'administrateur par défaut et le mot de passe sont connus. En fait, ces comptes par défaut peuvent être souvent trouvés sur Internet. Modifiez toujours l'identifiant de connexion et le mot de passe de l'administrateur par défaut en choisissant des identifiants que vous seuls connaissez. Pour l'accès administratif à votre point d'accès Wi-Fi, nous vous recommandons de désactiver l'accès sans fil et de demander une connexion réseau physique à l'aide d'un câble Ethernet. Si vous devez avoir des accès administratifs sans fil, désactivez l'accès HTTP et exigez l'accès HTTPS, qui prend en charge le chiffrement.

2. Une autre option que vous devrez configurer est le nom de votre réseau Wi-Fi (souvent appelé SSID). C'est le nom que vos appareils verront lorsqu'ils chercheront des réseaux Wi-Fi locaux. Donnez un nom unique à votre réseau pour pouvoir l'identifier facilement, mais assurez-vous qu'il ne contient pas de renseignements personnels. De plus, il ne sert pas à grand-chose de configurer votre réseau comme réseau Wi-Fi caché (ou non diffusé). Aujourd'hui la plupart des outils de balayage Wi-Fi ou tout agresseur qualifié peut découvrir facilement les détails d'un réseau caché. L'option recommandée est de laisser votre réseau Wi-Fi visible, mais sécurisé en utilisant les autres mesures visées dans ce bulletin d'information.

3. Ensuite, assurez-vous que seules les personnes que vous connaissez et à qui vous faites confiance peuvent se connecter à et utiliser votre réseau Wi-Fi et que ces connexions sont chiffrées. Vous devez vous assurer que les voisins ou les étrangers à proximité ne peuvent pas se connecter à ou surveiller

Protection de votre réseau à domicile

votre réseau Wi-Fi. Heureusement, ces dangers sont facilement atténués en activant tout simplement les paramètres de sécurité élevés sur votre point d'accès Wi-Fi. Actuellement, l'une des meilleures options à utiliser est le mécanisme de sécurité WPA2. En l'activant, le système demandera un mot de passe pour se connecter à votre réseau Wi-Fi, et une fois authentifié, ces connexions sont chiffrées. Veillez à ne pas utiliser des méthodes de sécurité plus anciennes, désuètes, comme la clé WEP ou même de n'avoir aucune sécurité du tout, ce qui est synonyme d'un réseau Wi-Fi ouvert. Un réseau ouvert permet à quiconque de se connecter à votre réseau Wi-Fi sans aucune authentification.

4. Lors de la configuration de votre mot de passe, assurez-vous qu'il est différent du mot de passe administrateur et qu'il ne peut pas être facilement trouvé ; nous recommandons des mots de passe d'au moins 15 caractères. Cela semble être un très long mot de passe, mais n'oubliez pas que vous ne devrez probablement le saisir qu'une seule fois pour chacun de vos appareils, qui vont le stocker, et s'en souvenir pour accéder au réseau à l'avenir. Si votre point d'accès Wi-Fi est dans un emplacement sécurisé physiquement et seulement accessible aux membres de votre famille, une option peut être d'enregistrer le mot de passe de l'utilisateur à l'arrière du point d'accès Wi-Fi afin de vous en rappeler facilement.

Ordinateurs et appareils multiples

Vous avez peut-être plus d'appareils, qui sont connectés à votre réseau domestique, que vous ne le pensez. Bon nombre de personnes pensent uniquement à leur ordinateur ou leur ordinateur portable, en oubliant les autres appareils présents chez eux comme les smartphones, tablettes, consoles de jeux, TV, ou même les babyphones. Assurez-vous que tous ces appareils sont connectés sur votre réseau à domicile, en toute sécurité, en changeant le mot de passe par défaut. Assurez-vous aussi que ces appareils disposent des correctifs et des dernières mises à jour.

De plus, pensez à utiliser des ordinateurs différents pour vos différentes utilisations informatiques chez vous. Par exemple, consacrez un ordinateur pour vos enfants ou les loisirs, comme pour jouer en ligne ou pour regarder des films. Ensuite, consacrez un second ordinateur plus sécurisé à vos activités bancaires ou hautement confidentielles. Enfin, votre fournisseur d'accès à Internet peut vous fournir également des services de sécurité gratuits et un logiciel avec votre abonnement Internet. Vérifiez auprès de votre fournisseur en consultant son site Internet.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse: securite.informatique@lausanne.ch

Lausanne

Piraté

Quelles que soient les précautions, quel que soit le soin que vous y apportez, votre ordinateur ou vos informations peuvent être compromis à un moment ou à un autre. Veuillez avertir immédiatement le service d'assistance ou l'équipe en charge de la sécurité dans ce cas. Plus vous signalez vite un incident, moins les criminels peuvent nuire.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse: securite.informatique@lausanne.ch

Lausanne

Piraté

Utiliser des ordinateurs connectés à l'Internet, c'est comme conduire une voiture, vous prenez des mesures pour vous protéger, mais un accident peut arriver à tout moment. Il en va de même avec la technologie. Vous prenez les mesures appropriées pour protéger votre ordinateur, mais votre ordinateur ou vos renseignements personnels peuvent être piratés. La clé pour vous protéger est de détecter et de réagir dès que possible à un incident. Si vous remarquez que quelque chose ne va pas et que vous réagissez rapidement, vous pouvez éviter de nombreux problèmes et gagner beaucoup de temps, pour vous, mais aussi pour notre entreprise. Voici quelques indicateurs communs que vous avez été compromis.

Vos comptes

L'une des premières méthodes pour détecter un problème, c'est en vous connectant à vos comptes, par exemple en faisant vos transactions bancaires en ligne, en ouvrant votre boîte de réception professionnelle, ou toute ressource qui requiert un identifiant de connexion et un mot de passe. Le premier signe d'un piratage potentiel : vous ne pouvez plus vous connecter, et votre mot de passe ne fonctionne plus. Si vous savez que vous utilisez le bon identifiant de connexion et le bon mot de passe, mais que malgré tout, vous ne parvenez pas à vous connecter, un cybercriminel peut avoir piraté votre compte et modifié votre mot de passe.

Si votre mot de passe ne fonctionne pas sur un compte professionnel, contactez immédiatement le service d'assistance ou la sécurité informatique pour recevoir de l'aide. Plus rapidement vous les contactez, plus vite ils peuvent réagir et stopper l'agresseur. Si ce n'est pas un compte professionnel, contactez les administrateurs du site Internet. Tous les sites Internet doivent indiquer un numéro de téléphone ou une adresse électronique de contact. Si vous croyez que votre mot de passe a été piraté, vérifiez si vous utilisez le même mot de passe sur tous les autres comptes. Si vous utilisez le même mot de passe, changez-le immédiatement.

Votre ordinateur

Votre ordinateur est la cible principale de nombreux criminels. Malheureusement, déterminer si votre ordinateur est attaqué n'est pas aussi simple que cela. Lorsque les ordinateurs sont piratés, ils tournent souvent au ralenti, plantent fréquemment, ou peuvent même redémarrer. Comment pouvez-vous savoir si votre ordinateur est piraté ou s'il fait simplement des siennes ? Voici quelques indicateurs fréquents :

- Votre antivirus génère une alerte. Votre logiciel antivirus doit analyser votre ordinateur chaque fois que vous enregistrez, ouvrez ou exécutez un fichier. S'il détecte un virus sur votre système, votre ordinateur peut avoir été piraté.
- Votre ordinateur vous dirige vers des sites indésirables ou des sites au hasard s'affichent sur votre

Piraté

écran, et vous ne pouvez plus les fermer. Les cybercriminels reprogramment parfois votre ordinateur pour vous diriger vers des sites Internet où vous ne souhaitez pas vous rendre.

- Vos amis ou vos collègues vous disent qu'ils reçoivent de drôles de messages de vos comptes Facebook, Twitter ou vos comptes de messagerie, et vous savez que vous n'avez pas envoyé ces messages. Cela peut également indiquer que ces comptes sont compromis.
- Vous pensez que vous avez installé par accident un logiciel suspect. Vous pouvez avoir cliqué sur un logiciel que vous ne souhaitiez pas installer et à présent, vous pensez que votre ordinateur est peut-être infecté.

Si vous pensez que votre ordinateur, votre appareil portable ou votre compte professionnel ont été compromis, ne tentez pas de résoudre le problème vous-même. Au lieu de cela, arrêtez d'utiliser cet appareil et contactez immédiatement le service d'assistance ou l'équipe en charge de la sécurité. Jouez la sécurité. Il vaut bien mieux signaler un système qui n'a pas été compromis que ne pas signaler un système qui a été compromis.

Le détecteur humain

Notre entreprise dispose d'une équipe de sécurité hautement qualifiée pour vous aider à vous protéger. Ces professionnels sont des experts qui comprennent les cybercriminels, plus précisément comment ils attaquent et ce qu'il faut faire pour se protéger contre eux. Cette équipe a contribué à la conception et a déployé plusieurs des technologies que nous utilisons, y compris les antivirus et les pare-feux. Notre équipe surveille constamment nos réseaux et recherche les dernières attaques menées contre notre entreprise.

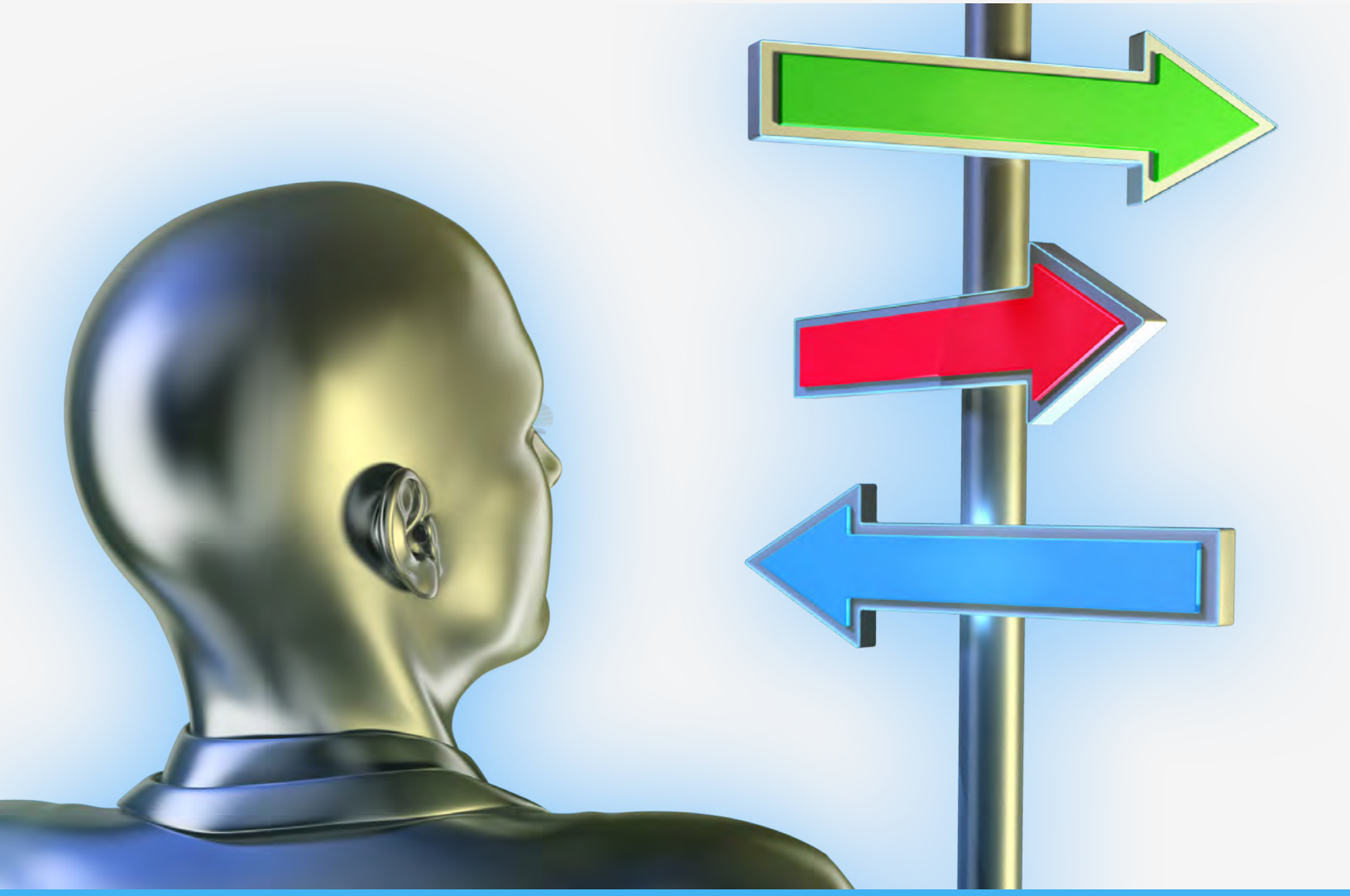
Cependant, notre équipe de sécurité ne peut pas toujours tout surveiller. Nous avons besoin de votre aide pour la protection de notre entreprise. Une manière d'aider notre équipe de sécurité est de les prévenir si vous pensez qu'un ordinateur est infecté ou si vous pensez que nos informations ont été perdues ou volées. Ce sont souvent des employés comme vous qui sont les premiers à voir ou à trouver que quelque chose ne va pas. Notre équipe de sécurité sera heureuse de vous entendre, car elle sait que vous faites tout pour l'aider.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse: securite.informatique@lausanne.ch

Lausanne

Éthique

L'éthique est la faculté de connaître la différence entre le bien et le mal et de prendre la juste et bonne décision. Si vous maintenez votre propre intégrité personnelle, non seulement vous êtes utile à notre entreprise ; mais de plus, vous vous construisez une réputation qui vous récompensera tout au long de votre carrière.



Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse: securite.informatique@lausanne.ch

Lausanne

Éthique

Notre entreprise promeut fermement l'idéal de pratiques équitables et éthiques. En outre, en adoptant une bonne éthique, nous serons moins susceptibles d'entrer en conflit avec la loi et plus susceptibles de conserver la fidélité de nos clients, de nos fournisseurs et de nos employés. Ainsi, nous attendons de tous les membres de notre entreprise, qu'ils travaillent de manière éthique. En termes simples, l'éthique est la faculté de connaître la différence entre le bien et le mal et de prendre la bonne et juste décision. Cela comprend le maintien de qualités d'intégrité personnelle, telles que l'honnêteté, l'équité et la sincérité. Maintenir votre propre intégrité personnelle au travail comprend le respect des directives suivantes :

- La tricherie, le vol et la tromperie sapent la confiance et ne seront pas tolérés. Quand vous ou l'entreprise affirmez que quelque chose va se passer, cet événement doit se produire. Si vous vous engagez envers quelqu'un en affirmant que vous pouvez faire quelque chose, puis que vous rencontrez un obstacle, contactez cette personne et expliquez-le lui.

- Les mensonges et les tromperies sont un véritable poison pour notre entreprise. Si vous ne connaissez pas la réponse à une question, dites-le, tout simplement. Sachez reconnaître quand vous ne savez pas ou quand vous ne pouvez pas répondre.

- Lorsque vous représentez notre entreprise, considérez les intérêts d'autrui. Cela ne veut pas dire donner à vos collègues, aux vendeurs ou à d'autres personnes tout ce qu'ils veulent. Mais cela signifie que vous êtes respectueux des autres, et que vous prenez le temps d'évaluer leurs besoins et même de discuter avec eux de votre processus de pensée, quand vous cherchez à résoudre un conflit entre eux et vous, ou notre entreprise.

- Vous devez respecter la vie privée des autres employés en n'essayant pas d'accéder à leur compte, ou ordinateur, de manière non autorisée. En outre, vous ne devriez pas intimider d'autres employés ou répandre des commérages ou des rumeurs à leur sujet.

- Vous devez poursuivre les intérêts de l'entreprise, et être dénué de motivations secrètes qui pourrait promouvoir d'autres organisations. En outre, vous devez de manière générale vous abstenir de dénigrer notre entreprise.

Éthique

Il n'est pas toujours facile de distinguer ce qui est bon et éthique dans chaque situation. Il peut y avoir des intérêts adverses et des points de vue divergents. Par exemple, une collègue pourrait vous demander d'envoyer un email indiquant qu'elle était présente au bureau alors qu'elle n'y était pas. Elle peut vous dire, par exemple, qu'elle a besoin de ce « petit mensonge » afin d'avoir un justificatif, pour sa compagnie d'assurance, qui prouve que sa voiture était dans le parking de l'entreprise quand elle a été emboutie. Il y a de bonnes méthodes pour résoudre des questions éthiques de ce type. Si vous ne savez pas ce qu'il faut faire, demandez de l'aide. Vous pouvez en obtenir en consultant les échelons supérieurs de la direction ou notre équipe juridique. Si vous maintenez votre propre intégrité personnelle, non seulement vous êtes utile à notre entreprise ; mais de plus, vous vous construisez une réputation qui vous récompensera tout au long de votre carrière.

Une éthique solide a des conséquences positives pour vous et notre organisation

Une bonne éthique consiste à s'assurer que nous bénéficions tous des avantages découlant d'un environnement de travail sûr basé sur la confiance et le respect mutuel pour tous les employés, les fournisseurs, les partenaires et les clients. Un environnement de travail solide et éthique nous permet de mener à bien nos missions sans coercition, sans intimidation et sans autres formes de harcèlement. Un milieu de travail éthique peut aussi vous protéger et protéger notre organisation au cas où des actions contraires à l'éthique ou des actions répréhensibles pénalement seraient commises par une autre personne, mettant en danger notre réputation. Les personnes comme vous jouent un rôle clé dans le maintien d'un programme éthique solide. Vos bonnes performances sont la preuve au jour le jour que le programme existe et fonctionne.

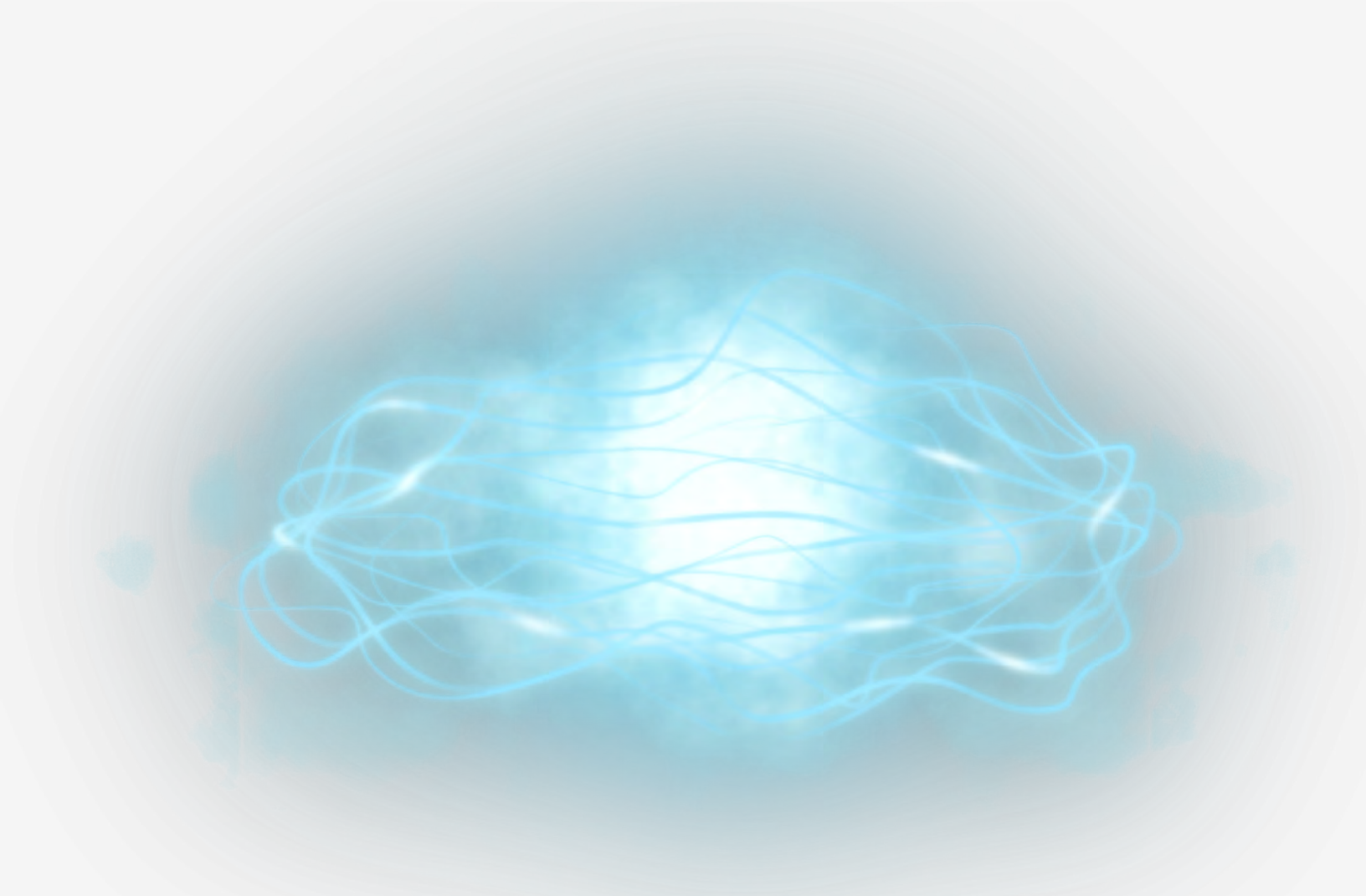
Si vous avez des questions sur ce qui est éthique ou non, ou si vous êtes dans une situation délicate, contactez votre supérieur ou notre équipe juridique. Nous sommes là pour vous aider.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse: securite.informatique@lausanne.ch

Lausanne

Le cloud

Les services cloud peuvent aider notre entreprise à être plus productive, mais ils s'accompagnent également de risques supplémentaires. Assurez-vous donc de suivre ces mesures dès que vous travaillez avec les services cloud.



Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse:
securite.informatique@lausanne.ch

Lausanne

Le cloud

Le cloud, ou le nuage, est une technologie puissante qu'utilise notre entreprise. L'informatique en nuage, ou cloud computing, consiste tout simplement à utiliser un fournisseur de services externe pour stocker, gérer ou traiter les données. La raison pour laquelle nous appelons ce service « le nuage » est qu'on ne sait jamais où nos données sont physiquement stockées, c'est un « nuage ». Des exemples de cloud computing incluent la création de documents sur Google Drive, le partage de fichiers via Dropbox ou le stockage de votre musique ou de vos photos sur iCloud d'Apple.

Solution

Les services cloud peuvent aider notre entreprise à être plus productive, mais ils s'accompagnent également de risques supplémentaires. Ainsi, veuillez vous assurer de suivre ces étapes chaque fois que vous travaillez avec les services de nuage informatique.

Permission

Veillez à avoir une autorisation avant d'utiliser les technologies de nuage informatique et veillez à utiliser uniquement les fournisseurs de nuage informatique agréés. Ne vous inscrivez pas, pour bénéficier d'un nouveau service, sans permission. Assurez-vous également de bien comprendre nos politiques indiquant les informations qui peuvent ou non être stockées dans le nuage, et les personnes avec lesquelles vous pouvez les partager.

Comptes personnels de services en nuage

Assurez-vous que toutes les données professionnelles ne sont jamais copiées ou stockées sur l'un de vos comptes personnels de nuage informatique, par exemple iCloud d'Apple ou votre compte Dropbox personnel. En outre, n'accédez pas à des comptes personnels de nuage informatique depuis des ordinateurs ou appareils professionnels, à moins d'avoir une autorisation préalable.

Mot de passe unique

Utilisez un mot de passe unique pour chacun de vos comptes de nuage informatique. Si votre service cloud prend en charge la vérification à deux étapes, nous vous recommandons vivement d'y avoir recours. Cela vous permet de bénéficier d'un niveau de protection supplémentaire. N'utilisez jamais le même mot de passe pour vos comptes cloud et pour vos comptes personnels.

Configuration

Par défaut, configurez votre compte de nuage informatique pour ne pas partager d'information ou de fichier avec n'importe qui. Ensuite, partagez seulement les fichiers avec des personnes ou des groupes de personnes ayant l'autorisation et ayant un besoin de connaître ces informations. Une fois qu'ils n'ont plus besoin d'accéder à ces fichiers ou à ces informations, supprimez leur accès aux données.

Antivirus

Veillez à scanner tout ce que vous téléchargez avec l'antivirus avant d'ouvrir un fichier. Étant donné que le nuage servira très probablement à stocker des fichiers partagés sur les ordinateurs d'autres personnes, ces

fichiers peuvent être infectés, car les autres personnes n'ont pas forcément le même niveau de sécurité que vous. Par exemple, une organisation partageait des fichiers par le cloud avec différentes personnes. L'une de ces personnes n'avait pas sécurisé son ordinateur, qui a été accidentellement infecté, ce qui a infecté tous leurs fichiers, y compris les fichiers partagés sur le cloud. Le virus a chiffré tous les fichiers, avant d'exiger que l'organisation paye une rançon pour les déchiffrer. Dans la mesure où ces fichiers étaient partagés sur le cloud, cela veut dire que tous les fichiers partagés des ordinateurs de toutes les personnes concernées ont été infectés et chiffrés.

Administration

Soyez attentif aux droits ou privilèges que vous accordez à d'autres personnes. Certains services de cloud computing vous permettent non seulement de partager des fichiers, mais aussi d'attribuer des droits d'administration à d'autres personnes. Cela signifie que vous pouvez donner aux personnes avec lesquelles vous partagez vos fichiers, la possibilité de permettre à d'autres d'y accéder ou de les modifier. Donnez seulement à ces personnes le minimum d'accès dont elles ont besoin pour faire leur travail. Si vous avez des questions sur les services cloud que vous pouvez utiliser pour le travail, sur les données qui peuvent être partagées, et sur les personnes avec lesquelles vous pouvez les partager, veuillez contacter votre supérieur ou l'équipe de sécurité des informations.

Partage de fichiers avec des liens

Le cloud est un outil extraordinaire pour le partage d'informations ; Cependant, vous pouvez facilement partager les mauvaises informations avec les mauvaises personnes (ou même avec tout Internet). Une caractéristique commune de certains services de cloud computing est la possibilité de créer un lien Web qui renvoie vers des fichiers ou des dossiers sur votre ordinateur. Cette fonction vous permet de partager ces fichiers avec toutes les personnes souhaitées, tout simplement en leur donnant un lien Web.

Le problème avec cette méthode, c'est qu'elle est très peu sécurisée. Toute personne qui connait ce lien a accès à vos fichiers ou à vos dossiers personnels. Si vous envoyez le lien à une seule personne, cette personne pourrait partager ce lien avec d'autres ou Google pourrait y avoir accès. Avant que vous ne vous en rendiez compte, n'importe qui pourrait alors accéder à vos fichiers. Si vous êtes autorisé à partager des données en utilisant un lien, assurez-vous de désactiver le lien une fois qu'il n'est plus nécessaire.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse: securite.informatique@lausanne.ch

Lausanne

Confidentialité

Le respect de la confidentialité consiste à protéger les informations personnelles d'autrui, non seulement pour respecter les exigences légales, mais aussi par respect pour autrui. Veuillez vous assurer de suivre les mesures décrites ici et dans notre programme de sécurité global, comme vous aimeriez que d'autres suivent ces mesures pour protéger votre confidentialité.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse:
securite.informatique@lausanne.ch

Lausanne

Confidentialité

Les progrès technologiques rendent plus facile que jamais l'accès aux informations et leur partage. Ils présentent cependant des défis énormes. Et cela est plus évident que jamais dans le domaine de la confidentialité individuelle et dans la gestion des informations personnelles des personnes. Dans le cadre de vos fonctions habituelles de travail, vous pouvez gérer des informations personnelles appartenant à autrui, comme le numéro de sécurité sociale, les informations financières, les dossiers scolaires ou les archives professionnelles, ou encore certains aspects de leurs dossiers médicaux et de santé.

Vous ne le voyez peut-être pas, mais des lois et des réglementations fédérales, étatiques et locales vous demandent de protéger la confidentialité des informations personnelles. Plus important encore : vous devez protéger ces informations dans le respect d'autrui. Vous devez prendre les mêmes mesures pour protéger la confidentialité des renseignements des personnes que vous le feriez pour protéger la confidentialité de vos propres renseignements. Voici quelques mesures à suivre pour permettre de protéger la confidentialité d'autrui :

Systèmes autorisés

Pour protéger la vie privée des personnes, vous devez uniquement utiliser des systèmes autorisés pour saisir, traiter ou stocker leurs informations. Ces systèmes ont de fortes mesures de sécurité en place, tels que les logiciels spécialisés de sécurité et des contrôles stricts sur la façon dont ils sont configurés et sur les personnes ayant un accès autorisé. Ne saisissez pas, ne traitez pas et ne stockez pas d'informations personnelles sur d'autres personnes sur des systèmes non autorisés, par exemple sur vos propres ordinateurs portables ou vos comptes de messagerie personnels.

Partage de données

Une autre mesure de protection des renseignements personnels consiste à s'assurer que seuls les membres du personnel autorisés y ont accès. Ces personnes doivent avoir reçu l'approbation préalable de la direction pour accéder à ces données. Elles doivent également avoir besoin de les connaître, ou en d'autres termes, elles doivent avoir besoin de l'accès aux données pour accomplir leur travail. La simple curiosité n'est pas un besoin suffisant pour justifier l'accès.

Cloud

Ne partagez ou ne stockez jamais d'informations sensibles sur des services publics Internet ou Cloud, comme Dropbox, Apple iCloud ou Google Drive, sans avoir reçu l'autorisation préalable de la direction.

Transfert de données

À certains moments, vous devrez peut-être transférer des renseignements personnels à des personnes autorisées. Le transfert de données s'accompagne de nombreux risques; elles peuvent se perdre, se faire voler ou même être interceptées. En tant que tel, vous ne devez utiliser que des méthodes sécurisées et autorisées qui prennent en charge le chiffrement lors du transfert de renseignements personnels d'une personne. Ne transférez jamais des données privées en utilisant des moyens insécurisés, comme par exemple votre propre compte de messagerie.

Confidentialité

Destruction des données

Une façon courante de compromettre des informations personnelles est liée aux mauvaises pratiques d'élimination de ces informations. Par exemple, quand vous jetez une vieille clé USB ou quand vous donnez des ordinateurs d'occasion, des informations personnelles sont souvent encore stockées sur ces appareils. Pour éviter ce danger, toutes les données fédérales sous format physique et électronique qu'il n'est plus nécessaire ou approprié de stocker doivent être correctement détruites, déchiquetées ou rendues illisibles. Pour les médias numériques, tels que les disques durs ou les clés USB, cela signifie qu'ils doivent être détruits physiquement ou effacés de manière sécurisée, ce qui garantit que les informations sont bien éliminées et ne peuvent pas être récupérées.

En protégeant la confidentialité d'autrui, vous aidez notre organisation à être conforme et vous faites preuve du respect que notre organisation montre envers autrui. Si vous avez des questions sur le type d'informations que vous devez protéger, sur la meilleure manière de les protéger, ou si vous pensez que nos informations ont été compromises, veuillez contacter le service d'assistance ou l'équipe de sécurité des informations.

L'impact de la technologie sur la confidentialité

La notion de confidentialité n'est pas nouvelle. Les organisations ont collecté et stocké des informations sur les individus depuis des siècles. Ce qui rend cette question si différente aujourd'hui, c'est la technologie. La technologie a non seulement permis aux organisations de recueillir beaucoup plus d'informations sur les individus, mais a également facilité le suivi d'individus spécifiques au fil des ans.

En outre, la technologie a également rendu beaucoup plus facile pour les personnes d'avoir illégalement accès à ces informations, de les copier et de les distribuer. C'est pourquoi il est devenu beaucoup plus difficile (et important) pour les organisations comme la nôtre d'identifier et de protéger activement toutes les informations personnelles que nous collectons. Vous jouez un rôle clé dans la protection des informations privées. C'est uniquement grâce à vos actions sécurisées que nous pouvons protéger la vie privée d'autrui.

Cette lettre d'information est publiée par le Service d'Organisation et d'Informatique de la Ville de Lausanne.
Pour plus d'informations, vous pouvez nous contacter à l'adresse: securite.informatique@lausanne.ch

Lausanne