Cybercriminalité

LUTTE CONTRE LA CYBERCRIMINALITÉ. GUIDE D'INFORMATIONS

Le Covid 19 ainsi que la fermeture des commerces non-essentiel ont accru l'usage d'internet. Il est recommandé de prendre conscience des risques et des moyens utilisés pour vous nuire et comment s'en protéger.

Le phishing / le Hameçonnage

« Je supprime directement les e-mails suspects sans les ouvrir »

Un mail vous parait suspect ? Il provient pourtant d'une banque (peut-être la votre) ? Ce mail vient d'une personne vous demandant de l'aide ? Ne faites jamais confiance à un e-mail provenant d'un inconnu. Vérifiez si l'adresse d'envoi ne contient pas de fautes d'orthographe et provient bien de l'entité qui vous écrit.

« Je vérifie si l'adresse du site web commence par HTTPS:// »

Si vous devez entrer des données confidentielles sur internet, un indicateur peut vous rassurer : Regardez en haut à gauche dans la case de l'URL si les lettres http sont suivies d'un s et précédées d'un cadenas. Cela signifie que le navigateur a établi une connexion sécurisée avec le site.

Les arnaques

« Je me garde de ne pas participer aux jeux concours que je reçois dans ma boite à e-mail »

On voit souvent des jeux concours gratuits sur internet, avec une multitude de lots alléchants à gagner. Ces jeux concours gratuits sur internet avec des lots alléchants à gagner ne sont parfois pas des marques qui cherchent à se faire connaître, mais bel et bien des entreprises qui gagnent de

l’argent en faisant ces concours. Il faut donc distinguer les deux.

Ne participez qu’aux concours organisés par des marques bien connues.

Utilisez une adresse e-mail dédiée aux concours.

Un concours gratuit ne demande jamais de transfert d’argent ou de vous acquitter des frais, c’est GRATUIT.

« Si je paie une facture reçue par e-mail, je passe toujours par le site web officiel de ma banque »

Connectez-vous directement sur le site de votre banque. Evitez de vous rendre sur des sites via un lien inscrit sur un autre site ou pire un e-mail. Evitez les pièces jointes ! Vous risquez via un lien de vous retrouver sur un faux site en pensant que c’est le bon. La vigilance est de mise.

Le détournement d’informations personnelles

« Un inconnu vient me parler sur les réseaux sociaux, je veille à ne pas lui répondre »

Les réseaux sociaux comme Facebook, Twitter et Instagram constituent une excellente façon d’être en contact avec la famille et les amis. Mais si vous n’êtes pas prudent lorsque vous êtes sur ces réseaux, les cybercriminels en profiteront pour tout savoir sur vous.

Assurez la confidentialité de vos renseignements personnels.

Évitez donc de partager :

- Des renseignements personnels.
- Des images qui révèlent des renseignements confidentiels : Avant de publier une image ou une photo, assurez-vous qu’elle ne contient pas de renseignements personnels.
- Des photos géolocalisées : La plupart des téléphones

intelligents et des caméras numériques indiquent automatiquement le lieu où une photo a été prise.
- Les « grandes » nouvelles : Les détails sur vos vacances (dates, photos, infos, …), les gros achats que vous avez réalisés ou les événements auxquels vous participez.
- Des renseignements bancaires et financiers : Il peut s'agir du nom de votre banque et de vos numéros de cartes bancaires.

« Je cache mon code secret lorsque j'utilise ma carte bancaire»

Il ne faut évidemment pas donner le code confidentiel de sa carte bancaire à tout le monde. Et lorsque vous tapez votre code, il est préférable de le faire à l'abri des regards.

- Surveillez vos comptes : Cela peut permettre de voir un vol avant que cela prenne des proportions plus dramatiques et que le voleur s'en donne à coeur joie dans ses achats.
- Evitez d'enregistrer vos données bancaires : Il est vrai que c'est pratique, on enregistre ses données bancaires sur des sites que l'on fréquente souvent pour gagner du temps lors du prochain achat. Le site garde en mémoire le numéro de la carte, la date de validité et même le cryptogramme.

La protection de mes données personnelles

« Je change 2 à 3 fois par an les mots de passe de mes comptes utilisateur »

Combinez les majuscules, les minuscules, les chiffres et les symboles.

Utilisez un mot de passe de plus de 13 caractères.

N'utilisez pas le même mot de passe pour chacun de vos comptes ni pendant plusieurs années.

Ne conservez pas vos mots de passe dans un endroit visible.

Ne communiquez jamais votre mot de passe à un tiers (via mail ou téléphone).

« J'utilise un antivirus sur mon smartphone »

Les virus circulent sur le web sous forme de liens avec des titres accrocheurs. Une fois qu'un virus s'est infiltré dans votre smartphone, il peut envoyer des messages indésirables à vos amis, s'emparer de vos renseignements personnels ou endommager votre appareil. Soyez donc toujours prudent lorsque vous êtes tentés de cliquer sur un lien dans les réseaux sociaux.

« Je vérifie les commentaires des applications pour smartphone avant de les télécharger »

Renseignez-vous sur les applications que vous installez. Sur l'App-store ou le Play-store, les autres utilisateurs peuvent l'évaluer et y laisser un commentaire. Lisez-en quelques-uns. Si c'est une application malhonnête, vous le verrez dans les commentaires. Tapez le nom de l'application sur votre moteur de recherche préféré, vous serez vite fixés.

« Ma banque me demande de vérifier mes informations en ligne via un e-mail, je veille à ne pas répondre et j'appelle ma banque »

Ne donnez jamais votre code pin ou d'autres codes bancaires par téléphone, email, sms ou médias sociaux. Appelez directement votre banque. En cas de fraude à la carte bancaire, avertissez immédiatement Card Stop au 070 344 344 afin de faire bloquer votre carte. Gardez un sens critique par rapport aux mails suspects qui vous proposent des choses trop belles pour être vraies, n'y réagissez pas.

Quelques liens supplémentaires qui pourront vous être utiles afin d'intensifier votre sécurité sur le web :

https://www.safeonweb.be
https://www.sfpd.fgov.be/fr/phishing
https://www.febelfin.be

Voici les 10 recommandations de Kaspersky (Grand acteur de la lutte contre la criminalité sur internet)

1. Limitez vos informations personnelles au cadre professionnel

Des employeurs potentiels ou prospects n'ont pas besoin de connaître vos relations personnelles ou l'adresse de votre domicile. Ils souhaitent en revanche identifier votre expertise et votre parcours professionnel, et savoir comment vous contacter. Vous ne communiqueriez tout simplement pas d'informations personnelles à des étrangers, alors ne les mettez pas à disposition de millions d'individus en ligne.

2. Activez vos paramètres de confidentialité

Les spécialistes du marketing tout comme les pirates informatiques adorent tout savoir sur vous. Ils peuvent en apprendre beaucoup à partir de vos habitudes de navigation et votre utilisation des réseaux sociaux. Mais vous pouvez gérer vos informations. Comme le fait observer Lifehacker, les navigateurs Web et les systèmes d'exploitation mobiles intègrent des paramètres permettant de protéger votre confidentialité en ligne. Les principaux sites Internet tels que Facebook proposent également des paramètres permettant de renforcer la confidentialité. Ils sont parfois (intentionnellement) difficiles à localiser parce que les entreprises souhaitent utiliser vos informations personnelles en raison de leur valeur marketing. Assurez-vous d'activer ces paramètres de protection de la confidentialité et de ne pas les désactiver.

3. Naviguez en toute sécurité

Vous ne prendriez pas le risque de vous aventurer dans un quartier dangereux, alors ne le faites pas en ligne. Les

cybercriminels utilisent du contenu tape-à-l'œil pour vous piéger. Ils savent que les gens sont parfois attirés par du contenu douteux et peuvent relâcher leur vigilance lorsqu'ils le recherchent. Le demi-monde d'Internet regorge de pièges difficiles à identifier. Un simple clic imprudent peut exposer vos données personnelles ou infecter votre appareil avec un programme malveillant. Ne pas céder à cette envie permet de ne laisser aucune chance aux pirates informatiques.

4. Vérifiez que votre connexion à Internet est sécurisée

Lorsque vous êtes sur Internet dans un lieu public, par exemple, à l'aide d'une connexion wifi publique, PCMag observe que vous n'avez aucun contrôle direct sur sa sécurité. Des experts de la cybersécurité d'entreprise s'inquiètent au sujet des terminaux, emplacements à partir desquels un réseau privé se connecte au monde extérieur. Votre connexion à Internet est votre vulnérabilité. Vérifiez que votre appareil est sécurisé et, en cas de doute, patientez (jusqu'à ce que vous puissiez vous connecter à un réseau wifi sécurisé) avant de communiquer des informations telles que votre numéro de compte bancaire.

5. Faites attention à ce que vous téléchargez

Les cybercriminels cherchent principalement à vous inciter à télécharger un programme malveillant, à savoir des programmes ou applications contenant des programmes malveillants ou tentant de dérober des informations. Ce programme malveillant peut se faire passer pour une application : jeu populaire, surveillance du trafic ou application météo. Comme le recommande PCWorld, ne téléchargez pas d'applications qui semblent suspectes ou qui proviennent d'un site Internet qui ne vous semble pas fiable.

6. Choisissez des mots de passe forts

Les mots de passe représentent l'une des vulnérabilités les plus importantes dans l'ensemble de la structure de sécurité Internet, mais il n'existe actuellement aucun moyen de les

contourner. Par ailleurs, le problème tient au fait que les gens choisissent généralement des mots de passe faciles à mémoriser (ex. « mot de passe » et « 123456 ») que les pirates peuvent également facilement deviner. Choisissez des mots de passe forts plus difficiles à décrypter pour les cybercriminels. Un logiciel de gestion des mots de passe peut vous permettre de gérer plusieurs mots de passe afin de ne pas les oublier. Pour garantir le niveau de sécurité d'un mot de passe, il doit être unique et complexe, à savoir contenir 15 caractères composés de lettres, de chiffres et caractères spéciaux.

7. Faites vos achats en ligne sur des sites Internet sécurisés

Chaque fois que vous réalisez un achat en ligne, vous devez fournir des informations de carte de crédit ou coordonnées bancaires, et ce sont précisément les informations que convoitent le plus les cybercriminels. Ne communiquez ces informations qu'à des sites qui proposent une connexion sécurisée et chiffrée. Comme le révèle l'université de Boston, vous pouvez identifier des sites sécurisés en recherchant une adresse qui commence par https: (S signifiant sécurisé) plutôt que http: Ils peuvent également être signalés par une icône représentant un cadenas à côté de la barre d'adresse.

8. Faites attention à ce que vous publiez

Internet ne possède pas de touche de suppression, comme l'a découvert un jeune candidat dans le New Hampshire. Tout commentaire ou photo que vous publiez en ligne peut le rester indéfiniment parce que la suppression de l'original (publiée sur Twitter, par exemple) ne supprime aucune des copies que d'autres personnes ont effectuées. Il n'existe aucun moyen de « supprimer » une remarque qui vous a échappé ou un selfie embarrassant que vous avez pris lors d'une fête. Ne publiez en ligne aucune information que vous ne souhaiteriez pas mettre à la disposition de votre mère ou d'un éventuel employeur.

9. Faites attention aux personnes que vous rencontrez en ligne

Les personnes que vous rencontrez sur le Net ne correspondent pas toujours à celles qu'elles prétendent être. En effet, elles peuvent même ne pas être réelles. Comme le signale InfoWorld, les pirates informatiques utilisent couramment des profils de réseaux sociaux factices pour se rapprocher d'internautes peu méfiants et vider leurs cyberpoches. Faites preuve de la même vigilance et prudence dans votre vie sociale virtuelle et réelle.

10. Mettez systématiquement à jour votre antivirus

Un logiciel de sécurité Internet ne peut pas vous protéger contre toutes les menaces mais il détectera et supprimera la plupart des programmes malveillants, mais vous devez, pour cela, veiller à ce qu'il soit à jour. Tenez-vous informé des mises à jour de votre système d'exploitation et des applications que vous utilisez. Elles représentent une couche de sécurité essentielle.