LA LETTRE DU CYBER-CONSEILLER

MAI ET JUIN 2023

NUMÉRO SPÉCIAL SÉCURITÉ

- Les arnaques sur le web et comment les éviter ?
- Qu'est-ce que le doxing et comment l'éviter ?
- Comment se protéger des ransomwares ?
- Créer un mot de passe fort
- Escroqueries avec AMAZON

La lettre Cyber, 16e année

LES ARNAQUES SUR LE WEB ET COMMENT LES ÉVITER ?

C'est quoi une arnaque ?

Une arnaque est une tentative d'obtenir un objet de valeur de manière frauduleuse, généralement de l'argent, mais pas nécessairement. Dans cet article, nous allons analyser les types d'arnaques en ligne les plus courants tout en vous donnant les outils et le savoir-faire dont vous avez besoin pour détecter les arnaques et vous en défendre. Protégez-vous ensuite en ligne avec un outil de cybersécurité fiable.

Que se passe t-il quand on se fait arnaquer ?

Les êtres humains tentent de s'arnaquer les uns les autres depuis que l'idée leur est venue d'attribuer une valeur aux objets et aux concepts. Lorsque quelqu'un met en œuvre un stratagème malhonnête pour vous soutirer de l'argent ou un autre objet de valeur, il s'agit d'une arnaque.

Avant de continuer, il convient de définir le terme d'arnaque et d'autres expressions pertinentes :

- Arnaque : stratagème malhonnête visant à vous convaincre de vous défaire d'un bien de valeur. D'autres termes équivalents sont « tromperie » ou « escroquerie ».
- Arnaqueur : personne qui tente d'en arnaquer une autre. L'arnaqueur peut également être appelé « escroc » ou, plus largement, « voleur ».
- Cible : personne visée par l'arnaque. Si l'arnaque aboutit, la cible devient une victime.
- Charmeur : type d'arnaqueur très particulier qui recourt à la ruse dans le but de manipuler ses cibles grâce à son charisme. Leurs arnaques sont généralement appelées « escroqueries de charme ».
- Stratagème : plan ou action de planifier une activité dont le but est de soutirer de l'argent à une cible.

Le développement et l'expansion d'Internet atteignant les dimensions que nous connaissons aujourd'hui, une nouvelle ère s'est ouverte pour les arnaqueurs. Lisez cet article pour découvrir les arnaques en ligne les plus répandues et apprendre à les éviter.

Les arnaques les plus courantes

L'arnaque de type phishing implique que l'arnaqueur (dans ce cas le « phisher », ou hameçonneur) se fasse passer pour une organisation légitime ou une personne de confiance pour contacter la cible et lui demander des informations personnelles sensibles telles que son numéro de compte, ses identifiants utilisateur ou les données de sa carte bancaire.

Ensuite, l'arnaqueur utilise ces informations pour voler de l'argent, usurper l'identité de la victime, ➡

➡

se livrer à des activités d'espionnage industriel ou à d'autres activités illégales. La grande majorité des arnaques de type phishing sont perpétrées par e-mail.

Le crowdsourcing offre une possibilité de demander des dons par Internet à quiconque se sent motivé à soutenir une cause. Il sert à financer des inventions, des idées commerciales, des projets créatifs ou couvrir des frais médicaux ou juridiques.
Les escrocs abusent des plateformes de crowdsourcing et mettent en place de fausses campagnes savamment conçues pour motiver ou émouvoir leur public cible. L'arnaqueur reçoit des dons qui peuvent être considérables, puis se volatilise.

L'arnaque dite « du prince Nigérian ».
Un individu se présente comme étant en contact avec une riche aristocrate emprisonnée, qui avait besoin d'argent pour financer sa libération. La cible reçoit la promesse d'un remboursement généreux à la libération de la prisonnière, qui bien entendu ne se matérialisait jamais.
Dans d'autres versions, l'arnaqueur demande une somme relativement modeste afin de débloquer le transfert de sommes bien plus importantes vers le compte de la cible. L'opération annoncée étant généralement juridiquement plus que douteuse, les cibles hésitent à signaler ce genre d'arnaque aux autorités.

L'arnaque au logiciel antivirus.
Des fenêtres contextuelles vous signalent que votre ordinateur a un besoin urgent d'une intervention pour se libérer d'un virus. Également connues sous le nom de scarewares, ces fausses publicités d'antivirus sont conçues pour vous faire paniquer et payer afin d'acquérir celle que vous croyez être la solution à tous vos tracas de malware. Mais il ne s'agit hélas que d'un mirage alors que votre argent, lui, disparaît dans les profondeurs d'Internet.

Comment savoir si l'on tente de vous arnaquer ?

En matière d'arnaques, la règle d'or est la suivante : Si c'est trop beau pour être vrai, c'est probablement que ce n'est pas vrai.

La prochaine fois que l'on vous fait une offre époustouflante, posez-vous les questions suivantes :

- Est-ce que je connais cette personne ? Souvent, les arnaques en ligne vous sont envoyées ou sont mises en œuvre par des contacts que vous ne reconnaissez pas. Cependant, d'autres sont fondés sur la confiance.
- Est-ce que cette offre est réaliste ? Encore une fois, faites confiance à votre instinct. Cet appartement est-il bien trop beau pour ce minuscule loyer ? Le prix de ce voyage de rêve est-il raisonnable ? On vous propose un job facile qui vous paie bien à ne rien faire ? On vous propose une récompense juteuse si vous acceptez de verser un acompte ? N'oubliez jamais le mantra anti-arnaque : si c'est trop beau pour être vrai, ce n'est probablement pas vrai.
- Cette transaction financière est-elle sûre ? Si vous êtes invité à envoyer un paiement, méfiez-vous des plateformes de paiement non protégées telles que les virements bancaires, Western Union ou les cartes-cadeaux. Ces paiements ne peuvent pas être remboursés, d'où l'intérêt pour les arnaqueurs. Méfiez-vous également des offres qui proposent le paiement par chèque bancaire. Les offres légitimes doivent accepter les méthodes de paiement standard réglementées, comme les cartes bancaires ou Paypal.
- Qu'est-ce qu'on me demande de révéler ? Les arnaques de type phishing collectent des informations personnelles qui pourront être utilisées contre vous par la suite. Aucune entreprise sérieuse ne vous demandera de confirmer vos identifiants de connexion, votre numéro de compte, votre numéro de carte bancaire ou des informations personnelles détaillées.
- Essaie-t-on de créer un sentiment d'urgence ? Les arnaqueurs tendent à créer un faux sentiment d'urgence pour vous forcer à prendre une décision précipitée. Certains font appel à l'angoisse de l'occasion manquée » pour vous presser de mordre à l'hameçon, tandis que d'autres vous menaceront de vous faire payer de lourdes pénalités si vous laissez passer un certain délai. Quoi qu'il en soit, une urgence extrême est un grand signe d'alerte à l'arnaque.
- L'histoire que me raconte cette personne a-t-elle un sens ? Si vous flairez l'arnaque au catfishing ou au charmeur, creusez dans son histoire. Recherchez-le ou la sur les réseaux sociaux et menez des recherches pour confirmer toutes les affirmations qu'il ou elle a faites. Toute incohérence est un signal d'alerte, répondez-y en conséquence.
- Tentent-ils de prendre contact en dehors de la plateforme ? Vous êtes protégé sur de nombreuses plateformes commerciales, de réservations ou sur les sites de rencontres dans la mesure où toutes vos communications ont lieu sur la messagerie du site. Les personnes qui demandent à vous contacter en privé par e-mail ou messagerie instantanée pourraient bien avoir quelque chose à cacher.

Que faire si vous êtes victime d'une arnaque ?

Coupez tout contact avec l'arnaqueur. Il ne va pas vous rendre votre argent, ce n'est donc pas la peine d'essayer de le convaincre.
Contactez immédiatement votre banque. Peut-être ne pourrez-vous pas récupérer l'argent que vous avez envoyé à l'arnaqueur, mais il ne vous coûte rien d'essayer.
Bloquez votre crédit. Si vous êtes victime d'une arnaque, bloquez immédiatement votre crédit pour éviter que les arnaqueurs n'ouvrent de nouveaux crédits en votre nom.
Modifiez vos mots de passe. Si vous avez révélé des informations personnelles sensibles à l'arnaqueur, soyez proactif et modifiez vos identifiants de connexion en ligne avec un mot de passe fort.

Comment se protéger des arnaques ?

Avant d'acheter quoique ce soit, faites une recherche sur l'entreprise et le site web. Quelle que soit l'urgence, même si vous mourez d'envie d'acheter l'article ou le service, faites d'abord votre recherche. Lisez bien les informations sur l'entreprise, les conditions d'utilisation et la politique de confidentialité (les sites web frauduleux tendent à n'en publier qu'une version très rudimentaire, voire aucune) et assurez-vous de bien vérifier la sécurité du site web avant de faire votre achat. Recherchez les avis des clients et voyez ce que d'autres ont à dire.

Payez par carte de crédit, si vous en avez une. Par rapport aux cartes bancaires et aux virements, les cartes de crédit sont beaucoup plus sécurisées. Votre fournisseur de carte de crédit sera forcément à vos côtés en cas de fraude, car c'est son argent, et pas le vôtre, qui est en jeu. En cas d'arnaque, vous pouvez bénéficier d'un remboursement.

Ne téléchargez jamais de pièces jointes et ne cliquez surtout pas sur les liens qui vous ont été envoyés par des contacts inconnus. Les arnaqueurs peuvent vous envoyer des malwares par le biais de pièces jointes et de sites Web. Par exemple, les chevaux de Troie tendent à s'infiltrer dans votre appareil par l'intermédiaire de pièces jointes à l'apparence inoffensive et sont souvent accompagnés de rootkits, de spywares ou d'adwares. Certains malwares se limitent à vous envahir de publicités, alors que d'autres peuvent être beaucoup plus nocifs. En règle générale, ne cliquez jamais sur un lien qui ne vous inspire pas confiance.

Gardez vos informations personnelles pour vous. De nombreux sites web vous demandent de répondre à des questions de sécurité pour récupérer votre mot de passe. N'oubliez pas ces réponses de sécurité et ne les partagez jamais. Dans le cas contraire, les arnaqueurs n'auront qu'à répondre à vos questions de sécurité à votre place. Bien entendu, cela s'applique également aux identifiants de connexion et aux numéros de comptes.

Assurez votre sécurité en ligne. Si un site Web propose une authentification à deux facteurs, utilisez-la. Ce système n'offre pas forcément une sécurité absolue, mais c'est un bon début. Utilisez des mots de passe forts et uniques sur les sites web que vous consultez et stockez-les de manière sécurisé par le biais d'un gestionnaire de mots de passe fiable.

QU'EST-CE QUE LE DOXING ET COMMENT L'ÉVITER ?

Le doxing consiste à exposer des informations sensibles et privées en ligne. Les pirates y ont recours pour se venger d'internautes, les harceler ou les menacer. Découvrez comment fonctionne le doxing et apprenez à préserver vos données. Ensuite, procurez-vous un logiciel spécialisé dans la protection des données pour vous assurer que vos informations d'identification en ligne restent protégées.

Comment fonctionne le doxing ?

Les auteurs de doxing épluchent les sites Internet à la recherche de petits éléments d'information sur une personne, puis les assemblent pour révéler la véritable identité qui se cache derrière un pseudonyme. Ces données peuvent inclure le nom de la victime, son adresse physique, son adresse e-mail, son numéro de téléphone, etc. Ils peuvent aussi acheter et vendre des informations sur le Dark Web.

Si beaucoup de gens pensent qu'Internet est anonyme, ce n'est pas du tout le cas. Il existe de nombreuses façons d'être identifié en ligne.

Le doxing via IP (ou via FAI) consiste à obtenir votre adresse IP, qui est liée à votre emplacement physique. Ensuite, l'auteur de doxing utilise des techniques d'ingénierie sociale pour inciter votre fournisseur d'accès à Internet (FAI) à lui divulguer davantage d'informations vous concernant.

En utilisant une application d'usurpation d'appel pour masquer son numéro de téléphone derrière celui du FAI, l'auteur de doxing peut appeler votre fournisseur et se faire passer pour un membre de son équipe d'assistance technique. Il peut alors utiliser votre adresse IP pour demander le reste de vos informations client.

Le doxing via les réseaux sociaux consiste à collecter des informations personnelles à partir de vos comptes sur les réseaux sociaux. Ces données peuvent inclure votre adresse, votre lieu de travail, vos amis, vos photos, ce que vous aimez et n'aimez pas, les lieux que vous avez visités, les noms des membres de votre famille et de vos animaux domestiques, etc.

Certaines de ces informations peuvent même fournir aux auteurs de doxing les réponses à vos questions de sécurité, qu'ils peuvent utiliser pour s'introduire dans vos autres comptes en ligne. C'est pour cela que vous devriez configurer tous vos comptes en mode privé.

Si vous êtes sur des plates-formes sociales en ligne telles que Reddit, WatsApp, Discord, YouTube ou autres, créez des noms d'utilisateur et des mots de passe différents sur chaque service.

Comment se protéger du doxing ?

De nombreux sites et applications vous encouragent à vous connecter à travers Facebook, Google, LinkedIn ou un autre service tiers. Le fait de se connecter à différents sites via son compte Facebook ou Google peut rendre particulièrement vulnérable à une violation de données. Si le mot de passe de votre compte fuite, un hacker peut accéder à tous les sites pour lesquels vous l'utilisez.

Vos profils sur les réseaux sociaux peuvent en dire long sur vous : emplacement (parfois même votre adresse complète), parcours professionnel, date de naissance, amis, famille, photos, intérêts, etc. En publiant autant d'informations sur Internet, vous vous exposez au doxing.

Lorsque vous créez de nouveaux comptes, choisissez un pseudonyme unique pour chaque service que vous utilisez. Si vous réutilisez un pseudonyme sur plusieurs sites, un auteur de doxing pourrait connecter vos comptes et les exploiter à la recherche d'indices sur votre identité.

Même si vos comptes n'ont jamais été piratés, un seul mot de passe ne suffit plus. Les pirates informatiques sont de plus en plus doués pour déchiffrer les mots de passe à l'aide de méthodes telles que l'enregistrement des touches et l'utilisation de mots de passe courants.

➡

➡

Etes vous victime de doxing ?

Si vous recevez des messages de menaces, du harcelement sur les réseaux sociaux, par e-mail, par téléphone, verrouillez tous vos comptes en ligne. Vérifiez si votre compte Facebook a été piraté et si votre compte Gmail est bien sécurisé. S'il est également bon de savoir si vos informations personnelles sont en vente sur le Dark Web, il n'est pas facile d'y accéder sans un logiciel spécial, comme le navigateur Tor.

COMMENT SE PROTÉGER DES RANSOMWARES ?

Le ransomware est une forme dangereuse de logiciel malveillant qui s'infiltre dans les ordinateurs et les appareils mobiles pour kidnapper des fichiers précieux et les garder en otage. Avec l'augmentation des attaques, il est essentiel que vous intégriez la prévention des ransomwares à votre vie numérique. Heureusement, il est facile (et essentiel) d'apprendre à se protéger contre les ransomwares.

Ce qui rend ce type de logiciel malveillant particulièrement dommageable, c'est sa capacité à détruire, corrompre ou verrouiller les fichiers de ses victimes. Nous parlons bien plus que de perdre de précieuses photos de famille ou des documents comptables de plusieurs années , qui sont bien entendu des pertes dévastatrices.

Les cyberpirates s'intéressent principalement à l'argent facile et aux paiements rapides qu'offrent les ransomwares, mais leurs attaques vont au-delà du simple vol. Une fois que leur logiciel malveillant a infecté votre ordinateur ou votre appareil mobile, toutes vos informations, notamment les numéros d'identification personnels, les noms d'utilisateur et les mots de passe risquent d'être volés ou exposés. Si, comme la fameuse souche WannaCry, le ransomware a des propriétés virales, chaque appareil présent sur votre réseau est en danger.
Peu importe l'appareil que vous utilisez : les Mac, les iPhones, les iPad, les PC Windows et les appareils Android sont tous vulnérables aux attaques de ransomwares,

Moyens de protection

- Choisir un logiciel antivirus efficace.
- maintenir votre logiciel antivirus à jour.
- Se méfier des demandes d'installation dans des fenêtres contextuelles. La prochaine fois que vous vous trouvez sur un site vous informant que vous devez installer, par exemple, une mise à jour pour Adobe Flash pour afficher le contenu d'un site, allez chercher la dernière version directement à la source. Ce conseil s'applique à toutes les fenêtres contextuelles de mise à jour de logiciel.
- Réfléchissez à 2 fois avant de cliquer sur un lien. Ne cliquez pas sur les liens que vous recevez de contacts inconnus par SMS, e-mail ou applications de messagerie telles que Skype ou WhatsApp. Même si vous pensez connaître l'expéditeur, examinez de plus près son adresse et le lien lui-même avant de poursuivre. Si quelque chose vous semble suspect, abstenez-vous.
- Ne téléchargez pas d'applications depuis des sources inconnues, mais à partir de sources fiables telles que Microsoft Store, Apple Store et Google Play Store, et évitez les magasins d'applications tiers.
- La meilleure façon de prévenir la perte de données est d'utiliser une combinaison de méthodes de stockage hors ligne et en ligne. Enregistrez vos fichiers le plus fréquemment possible sur un ou plusieurs appareils physiques (par exemple disques durs externes, clés USB, cartes SD) et sur des services de stockage cloud (par exemple Dropbox, Box, Google Drive).
- Aussi ennuyeux que puissent être les avis de mise à jour du système Windows, Apple et Android, vous ne devez jamais les ignorer. Un grand nombre de ces mises à jour impliquent des correctifs de sécurité essentiels pour empêcher les ransomwares et autres programmes malveillants d'infiltrer vos appareils. Si vous utilisez un système d'exploitation ancien que Microsoft ne prend plus en charge, notamment Windows XP, vous êtes particulièrement vulnérable en cas d'attaque.

Faut-il payer la rançon ?

Non, vous ne devez absolument pas payer la rançon, ni essayer de négocier avec les criminels à l'origine de l'attaque. En effet vous n'avez aucune certitude de récupérer vos fichiers. Malgré des apparences honorables destinées à inspirer confiance à leurs victimes, il n'y a pas d'honneur parmi les cyber-voleurs.

COMMENT CRÉER UN MOT DE PASSE FORT ?

Le meilleur mot de passe est un mot de passe fort, mais vous n'êtes pas le seul à avoir du mal à trouver de bons mots de passe. Un mot de passe inviolable empêche les pirates de s'introduire dans vos comptes et appareils, tout en protégeant vos comptes et vos données personnelles.

Le piratage de mots de passe est une activité lucrative, et si vous utilisez le **même mot de passe depuis des années** et sur plusieurs sites, il est probable qu'il ait déjà été compromis. Dans le cadre d'une violation de données, les pirates volent les identifiants d'utilisateur, compilent toutes les informations dans une énorme liste, puis la vendent à d'autres cybercriminels qui l'utilisent à leurs propres fins.

Anatomie d'un mot de passe sûr.

Evitez les mots de passe trop simples

N'utilisez pas de mots de passe trop évidents ou trop typiques. Voici une petite liste des types de mots de passe à éviter :

- Séquence de chiffres ou de lettres (« abcde », « 12345 »...).

- Mot de passe comportant tout ou partie de votre nom.
- Mot de passe comportant des informations personnelles (date d'anniversaire, lieu de naissance...).
- Série de caractères répétitifs (« aaaaa », « 0000 »...).
- Le mot « mot de passe » (ou « password »). Aussi invraisemblable que cela puisse paraître, il y a toujours des gens qui utilisent ce type de mots de passe.

Votre mot de passe ne devrait comporter aucune information personnelle. En allant sur les médias sociaux, les pirates peuvent facilement recueillir des informations sur n'importe qui, et les utiliser dans leurs tentatives de piratage.

Contrez les attaques par force brute

Les attaques par force brute utilisent une combinaison de caractères après l'autre pour finalement générer celle que vous avez choisie comme mot de passe. Voici comment vous préserver de cette technique :

- Utilisez 15-20 caractères ou plus. Plus un mot de passe est long, plus il est fort. Chaque caractère supplémentaire augmente les combinaisons potentielles de mot de passe, ce qui prolonge considérablement le temps nécessaire à une attaque par force brute.
- Utilisez plusieurs types de caractères. Ce n'est pas pour rien que de plus en plus d'organisations exigent des mots de passe composés de lettres majuscules et minuscules ainsi que de symboles et de chiffres. Lorsque vous incluez tous les types de caractères possibles, vous maximisez le nombre de possibilités par caractère, ce qui rend votre mot de passe difficile à pirater.
- Évitez les caractères de substitution courants. Les pirates programment leur logiciel de cracking pour qu'il tienne compte des échanges de caractères typiques (comme « 0 » lieu de « O »). « 410|\|3 » est aussi facile à craquer que « ALONE ».
- Évitez les suites de touches de clavier. Les chemins de clavier faciles à mémoriser (comme azerty ou qsdf) ne sont pas plus difficiles à pirater que des mots ordinaires. Ce type de mot de passe est loin d'être sûr.

La méthode de la phrase obscure.

Cette technique reprend l'approche de la phrase de passe et l'élève de quelques crans en matière de sécurité.

Déjouez les pirates en choisissant des mots peu courants, tels que des noms propres, des noms de personnages historiques, des mots archaïques ou même des mots dans d'autres langues.

Pour mémoriser plus facilement votre nouvelle phrase de passe, vous pouvez construire une histoire à partir des mots que vous choisissez. Pensez à quelque chose que vous n'oublierez pas, de sorte que vous n'aurez pas à récupérer les mots de passe que vous avez oubliés.

Pour rendre votre mot de passe encore plus fort, ajoutez des caractères spéciaux (autres que de le tiret du bas) entre les mots. Vous pouvez également remplacer des lettres par des caractères, mais évitez les substitutions courantes.

Regardez cette phrase de passe : *SunTzu-cheesesteak-transistor-Noël-obrigado*. Le grand stratège militaire Sun Tzu avait peut-être un tel penchant pour les sandwichs au fromage qu'il a reçu pour Noël un appareil à fromage alimenté par un transistor, pour lequel il a exprimé ses remerciements en portugais.

La méthode de la phrase

Créée par un expert en cybersécurité, la méthode de la phrase consiste à transformer une phrase en mot de passe à l'aide d'une règle que vous créez vous-même. Par exemple, vous pouvez extraire les deux premières lettres de chaque mot de votre phrase, puis les enchaîner pour créer un mot de passe.
« Nebraska est le meilleur album de Bruce Springsteen » devient alors : *NeeslemeialbBrSp*.

Authentification à 2 facteurs

Devenue une pratique de sécurité standard, l'authentification à deux facteurs (2FA) et son cousin élargi l'authentification à plusieurs facteurs (MFA) ajoutent des couches de protection supplémentaires à votre connexion.
Si un pirate obtient votre mot de passe, il devra surmonter au moins un obstacle supplémentaire avant de pouvoir accéder à vos données.
Parmi les mesures d'authentification courantes, on retrouve les codes envoyés par SMS, les applications d'authentification mobile, le scan des empreintes digitales ou faciales, ou encore un jeton physique. Mais comme les pirates peuvent usurper ou intercepter des SMS, nous ne recommandons pas les SMS comme méthode 2FA.

Les clés de sécurité

Les clés de sécurité physiques font partie des méthodes MFA les plus sûres.

Disponibles en plusieurs versions (USB, NFC et Bluetooth), elles ne donnent accès qu'au détenteur de la clé. De cette manière, elles sont beaucoup plus sûres que la vérification par SMS, à condition que vous ne perdiez pas votre clé.

LES ESCROQUERIES LES PLUS COURANTES AVEC AMAZON

Aucun site web n'est totalement à l'abri des escroqueries, et Amazon ne fait pas exception. Amazon est une plateforme mondiale de confiance, et les escrocs profitent de son utilisation très répandue au moyen d'escroqueries téléphoniques, de faux e-mails, d'arnaques Amazon Prime et de faux sites web.

1-Escroqueries Amazon Prime

Le service de streaming vidéo d'Amazon est une cible de choix pour les fraudes, notamment à l'occasion de l'Amazon Prime Day, où les offres et les remises abondent pour les membres Prime. Voici quelques-unes des formes que peuvent prendre les escroqueries :

➡

➡

Promotions Prime Day

Les membres d'Amazon Prime s'attendent à recevoir des promotions de la part d'Amazon à l'occasion du Prime Day, et les escrocs en profitent. Dans cette arnaque, les membres de Prime reçoivent des SMS qui annoncent des offres. Mais les liens contenus dans ces SMS ou e-mails renvoient à des sites web frauduleux qui peuvent dérober leurs données personnelles ou informations de paiement.

Erreurs de paiement

Les utilisateurs reçoivent un e-mail ou un SMS, souvent avec une fausse adresse IP prétendant provenir d'Amazon, les informant qu'ils doivent mettre à jour leurs informations de paiement pour leur compte Amazon Prime. Il s'agit d'une arnaque Amazon courante, avec de nombreuses variantes.

Problèmes d'activation

Lorsque les membres Prime rencontrent des difficultés pour accéder au contenu d'Amazon Prime, ils se tournent souvent vers Google afin de trouver la solution. Une arnaque Amazon Prime consiste à publier un faux numéro de téléphone sur un site web frauduleux convaincant. Quand l'utilisateur pense appeler le service d'assistance d'Amazon Prime, l'escroc essaie de l'inciter à payer pour activer son compte Amazon Prime.

2-Escroqueries de phishing Amazon

Elles reprennent souvent les graphismes et autres éléments de design des véritables e-mails d'Amazon, ce qui les rend tout à fait crédibles. Les e-mails de phishing Amazon se présentent sous plusieurs formes et comprennent habituellement un lien vers un site web usurpé où la victime est invitée à effectuer un paiement ou à saisir des informations personnelles. Voici les types de messages les plus courants figurant dans les e-mails de phishing Amazon :

Mise à jour de vos modalités de paiement

Les e-mails de mise à jour de vos modalités de paiement tentent de vous persuader que vos informations de paiement Amazon doivent être mises à jour ou ont expiré.

Vous avez gagné !

Certaines escroqueries par phishing Amazon font miroiter un prix à leurs victimes pour les inciter à cliquer sur un lien vers un site Amazon falsifié.

Confirmation de commande

Les arnaques à la confirmation de commande prennent la forme d'un e-mail ou d'un SMS contenant un lien infecté demandant aux clients de vérifier un achat récent.

3-Escroquerie à la carte cadeau

Demander une carte cadeau Amazon comme mode de paiement est une escroquerie courante qui pousse la victime à acheter une carte cadeau Amazon, puis à divulguer son numéro à l'escroc. Voici comment débutent souvent les escroqueries à la carte cadeau Amazon :

Assistance urgente

L'escroc se fait passer pour un ami ou un membre de la famille et demande une aide urgente sous la forme d'une carte cadeau Amazon.

Support technique

Dans ce type d'escroquerie, une personne se faisant passer pour un agent du service technique d'Amazon convainc la victime qu'elle doit mettre à niveau un abonnement ou acheter un service en utilisant une carte cadeau Amazon comme moyen de paiement.

Récompense liée à une enquête

Les escrocs proposent des cartes cadeaux Amazon comme récompense en échange de la participation à une enquête. Ils recueillent vos informations personnelles sensibles dans les réponses à l'enquête.

Paiement d'une dette

Les victimes reçoivent généralement un appel prétendant qu'elles ont une dette impayée, par exemple une pénalité fiscale, et leur demandant de la régler en utilisant une carte cadeau Amazon. En dehors de l'achat de produits sur le véritable site web d'Amazon, personne ne peut légitimement demander un paiement au moyen d'une carte cadeau Amazon.

Si vous n'êtes pas sûr qu'un SMS ou un e-mail concernant une carte cadeau Amazon soit authentique, vérifiez le numéro de téléphone et le lien d'enregistrement. Les vraies cartes cadeaux Amazon portent le numéro 455-72, et le lien d'enregistrement doit comprendre amazon[point]com/g/ suivi du code de validation.

4-Faux sites web Amazon

De nombreux messages d'escroquerie Amazon contiennent des liens vers des pages web imitant les vraies. Ces sites présentent des différences presque indétectables par rapport au véritable site Amazon, faisant croire aux victimes qu'elles peuvent effectuer des achats et saisir des informations de paiement en toute sécurité. Les achats effectués sur de faux sites Amazon ne seront jamais livrés. Vérifiez toujours la sécurité et l'authenticité du site web avant l'achat.

Même si le nom « Amazon » figure dans l'URL, il peut ne pas s'agir d'un site Amazon légitime. Pour vous assurer qu'il s'agit bien du vrai site, vérifiez la présence du point dans ***amazon.com*** ou ***amazon.fr***.

5-Escroqueries à l'échec de livraison

Les escroqueries liées aux échecs de livraison et à l'envoi d'articles visent les vendeurs d'Amazon plutôt que ses clients. Le destinataire de la commande affirme frauduleusement ne pas avoir reçu son achat et demande un remboursement ou l'envoi d'un second colis. Il s'agit d'une fraude relativement ancienne, mais dont les vendeurs Amazon doivent être avertis.

6-Escroqueries aux faux prix

Les escrocs utilisent souvent des messages électroniques ou des SMS pour informer le destinataire qu'il a gagné un prix. Le message comprend généralement un lien infecté ou mène à une enquête à laquelle le destinataire doit répondre pour réclamer son prix. L'enquête incite ensuite la victime à fournir des informations sensibles à l'escroc.