mon jardin numérique

Ateliers informatique & Internet

Nom :

Prénom :

Lieux :

Formateur :

Les arnaques sur internet

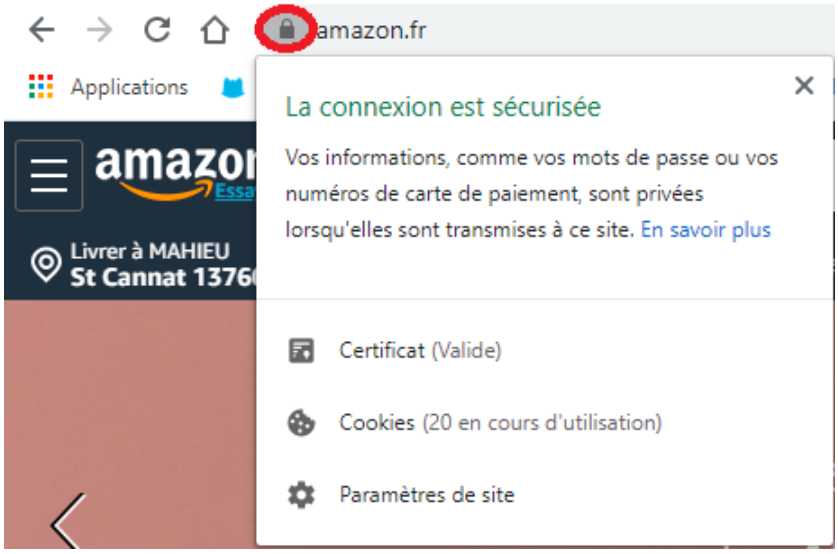
Mon Jardin Numérique
Espace Valentine – Bât. B – 1, montée de Saint Menet - 13011 Marseille
Tél. 04 91 08 31 91
contact@m-j-n.com

SAVOIR SI UN PAIEMENT EN LIGNE EST SÉCURISÉ

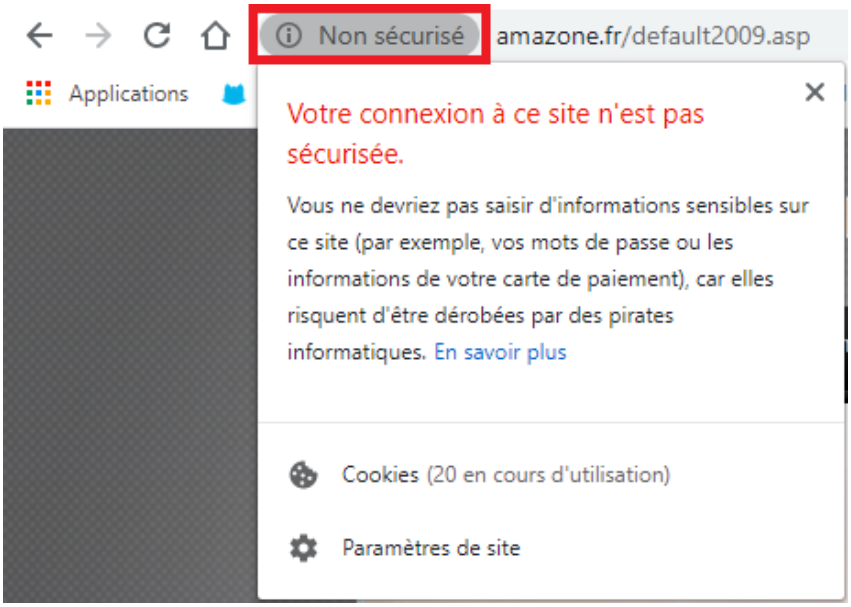
Le site e-commerce doit être muni d'un encodage **SSL (*Secure Sockets Layer*)** qui va permettre de **crypter les données personnelles** fournis. Lors du paiement en ligne, l'url dans la barre d'adresse doit être la suivante : **« https://.... »** (Valable pour Firefox et Edge. Cliquer deux fois sur l'url dans Chrome pour le voir apparaître). Le symbole d'un cadenas doit aussi apparaître dans la barre d'adresse du site e-commerce. Ces deux signes permettent de confirmer que la plateforme en ligne est fiable. On peut donc effectuer le paiement en ligne en toute sécurité. Bien sûr, il est également essentiel de connaître la popularité de la boutique en ligne où l'on veut effectuer l'achat. Payer en ligne sur la fnac.com sera plus sécurisant que sur un site moins connu. Tous ces conseils permettront de limiter les risques de toute sorte de piratage sur internet.

Exemple :

- Site sécurisé (Les informations que l'on va rentrer seront cryptées) :



- Site non Sécurité (Les informations que l'on va rentrer ne seront pas cryptées) :



En cas de doute, cliquer sur ou , permet de vérifier si la connexion au site internet est sécurisée ou non (comme ci-dessus).

LES DIFFÉRENTS MOYENS DE PAIEMENT

Payer en ligne avec sa carte bancaire, sur un site de **e-commerce**, est un moyen simple et efficace de faire ses achats. Cependant, il existe un risque de se faire pirater les données personnelles, en fournissant les chiffres de la carte bancaire, lors de l'achat. Heureusement, il existe de nombreuses alternatives.

⇨ E-carte bancaire

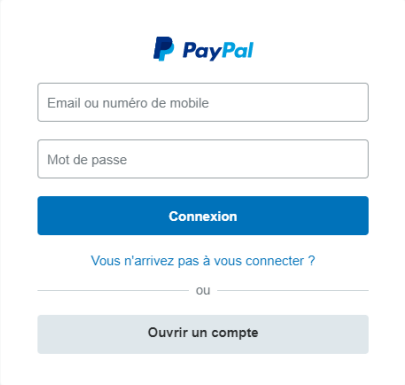
Cette méthode de paiement permet de générer une **carte virtuelle éphémère**, les banques proposent en général cette fonctionnalité gratuitement.
Lors d'un achat, il suffit d'utiliser l'application ou le site de la banque, pour entrer le montant souhaité à mettre sur cette carte virtuelle et sa durée de validité. L'obtention d'un numéro de carte à usage quasi unique permet de conclure l'achat sans communiquer les coordonnés bancaires en ligne.

⇨ Paypal

C'est une des solutions de paiement les plus connues aujourd'hui. Elle est proposée par une grande majorité des E-commerçants. La popularité de **Paypal** est notamment fondée sur sa facilité d'utilisation.

1. Il faut commencer par ouvrir un compte, seules quelques informations suffisent.
2. Enregistrer une carte ou un compte bancaire.
3. Au moment de payer, il suffit de cliquer sur le lien renvoyant au site Paypal, de se connecter à l'aide de l'adresse Email et du mot de passe, et enfin, de valider le paiement.

1.



2.

3.

⇨ 3D Secure (carte bancaire)

Le protocole **3D Secure** est parfois utilisé par les sites **e-commerce**, afin de valider la transaction. Quand un paiement **3D Secure** est proposé, les étapes sont :

1. Saisie des renseignements demandés dans le cadre d'un paiement classique par carte (numéro, Nom du titulaire, date de validité de la carte, Cryptogramme visuel au dos de la carte)
2. réception d'un SMS contenant un code d'authentification
3. saisie du code sur le site
4. validation du paiement

⇨ Carte prépayée

La carte bancaire prépayée est avant tout une carte de paiement. Elle fonctionne de la même manière que n'importe quelle carte bancaire Visa ou Mastercard. Elle permet de retirer de l'argent, ou de payer sur Internet ou en magasin en France ou à l'étranger. Elle garantit une certaine sécurité lors d'achats sur internet, du fait qu'elle ne soit pas rattachée à un compte en banque. La plupart des points de vente physiques permettant de trouver une carte bancaire prépayée sont les buralistes. Il est possible de la recharger par virement bancaire, depuis votre compte principal, ou chez les buralistes.

LES DIFFÉRENTES MENACES SUR INTERNET

⇨ Le phishing ou hameçonnage

Il s'agit d'une méthode permettant de récupérer des données d'une victime en lui faisant croire qu'elle utilise **un site**, **une application** ou **un service** qu'elle connaît. Dans la majeure partie des cas ces données sont privées et sensibles.
Comment détecter les tentatives de hameçonnage et s'en prémunir ?

- Connaître les **réelles** habitudes des entreprises : Certaines grandes entreprises indiquent clairement ne **jamais** faire des demandes comme la mise à jour d'informations de sécurité par e-mail.
- Toujours vérifier **l'URL** du site web en question avant de communiquer des informations sensibles : Le nom du site web que l'internaute est supposé visiter peut être légèrement différent**,** l'extension peut changer**,** une lettre peut être ajoutée dans le nom etc.
- Vérifier la présence de **fautes d'orthographe** : Bien souvent la détection de fautes d'orthographe répétées suffit à déceler une tentative de hameçonnage.
- Vérifier la source : Si un e-mail est reçu demandant d'accéder au site pour exécuter telle action, vérifier que l'expéditeur soit connu. Attention aux **adresses mail falsifiées.**

Et si ça m'arrive ? Il faut changer le plus vite possible les données transmises

⇨ Les Exploit kits (kits d'exploitation)

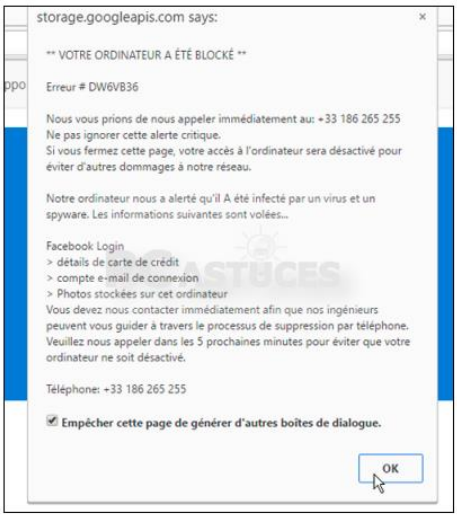
Des vulnérabilités, il y en a partout, même dans votre **navigateur** ! Et les exploiter est leur but. Les exploit kits se cachent dans des pages web malveillantes en attendant les internautes qui les visitent avec des versions de logiciel ou de navigateur non mises à jour (et vulnérables).
Comment s'en protéger ? Toujours **METTRE A JOUR** les logiciels et extensions de navigateur !

⇨ Le malvertising

Il s'agit de l'exploitation de la publicité. L'exemple classique est l'utilisation d'une publicité anodine, qui se transforme ensuite en publicité malveillante. Vous avez peut-être déjà connu le cas de la fenêtre pop-up difficile à fermer sur votre smartphone ou ordinateur.
Exemple :

1.

2.



Si cela vous arrive :

- ✓ sur ordinateur, forcer l'arrêt du navigateur (CTRL+ALT+Suppr, ouvrir le gestionnaire des tâches, cliquer sur le nom de l'application et fin de tâches) et ne jamais appeler le numéro de téléphone indiqué.
- ✓ Sur smartphone, aller dans le gestionnaire d'applications actives et fermer l'application.

Installer un bloqueur de publicités pour éviter les pubs intempestives (Adblock plus, Ublock …).

LES MALWARES

⇨ Qu'est-ce qu'un Malware ?

Les **malwares**, ou « **logiciels malveillants** » sont des programmes malveillants qui peuvent être nocifs pour les systèmes. Hostiles, intrusifs et intentionnellement méchants, les malwares cherchent à envahir, endommager ou mettre hors service les ordinateurs, les systèmes informatiques, les tablettes ou les appareils mobiles.

⇨ Comment savoir si je suis victime d'un malware ?

Les malwares se manifestent par des comportements inhabituels variés :

- Votre ordinateur ralentit.
- Un raz-de-marée de publicités indésirables déferle sur votre écran. Des pop-ups qui apparaissent soudainement sont un signe d'infection par un malware.
- Votre système plante régulièrement, se bloque ou affiche un écran bleu, ce qui peut se produire sur les systèmes Windows après une erreur fatale.
- Vous remarquez une étrange perte d'espace de stockage, probablement due à un malware envahissant qui se cache sur votre disque dur.
- Etc …

⇨ Comment s'en protéger ?

Si vous pensez être victime d'un malware, ou souhaitez simplement être prudent, voici les étapes à suivre.

- Analyser tous les fichiers téléchargés provenant de sources inconnues à l'aide de l'antivirus.
- Utiliser un antivirus à jour.
- Utiliser des logiciels qui permettent d'analyser votre système et d'éradiquer les malwares (Malwarebytes, ADWcleaner …).
- Réinitialiser son navigateur.
- Effectuer des sauvegardes de disque dur.

LES DIFFÉRENTES FAMILLES DE MALWARES

⇨ Les virus

Un virus est un programme écrit pour s'introduire dans votre ordinateur et endommager ou altérer vos fichiers ou vos données. Un virus a la capacité de corrompre ou de supprimer des données de votre ordinateur.

⇨ Les spywares

Un spyware est un type de programme qui s'installe sur un ordinateur personnel, avec ou sans permission, afin de collecter des informations sur l'utilisateur, son ordinateur ou ses habitudes de navigation, de suivre tout ce qu'il fait sans qu'il le sache, et d'envoyer ces données à un utilisateur distant.

⇨ Les chevaux de troie

Un cheval de Trois n'est pas un virus. C'est un programme de destruction qui a l'apparence d'une application légitime. À l'inverse des virus, les chevaux de Troie ne se répliquent pas eux-mêmes, mais ils peuvent être tout aussi destructeurs. Les chevaux de Troie ouvrent également une porte d'entrée clandestine dans votre ordinateur pour donner l'accès à des programmes ou utilisateurs malveillants, ce qui leur permet de dérober vos informations personnelles et confidentielles.

⇨ Les vers

Les vers sont des programmes malveillants ayant la capacité de se répliquer eux-mêmes sans cesse sur un disque local, des partages réseau, etc. Le seul objectif d'un ver est de se répliquer encore et encore.

Il n'altère aucune donnée ou aucun fichier sur l'ordinateur. En raison de sa faculté à se répliquer, il occupe beaucoup d'espace sur le disque dur et consomme plus de ressources de processeur, ce qui rend l'ordinateur plus lent.

⇨ Les logiciels publicitaires

De manière générale, un logiciel publicitaire désigne une application logicielle dans laquelle des bannières publicitaires s'affichent pendant l'exécution d'un programme. Le logiciel publicitaire peut se télécharger automatiquement sur votre système lors de la visite d'un site web et être visualisé dans une fenêtre contextuelle ou dans une barre qui apparaît automatiquement à l'écran. Ces logiciels publicitaires sont utilisés par les entreprises à des fins marketings.

⇨ Les spams

L'envoi de spam est une méthode visant à submerger Internet avec des copies d'un même message. La plupart des spams sont des offres publicitaires envoyées aux utilisateurs sous la forme d'un message électronique non sollicité. Les spams sont aussi appelés courrier indésirable. Ces messages de spam sont très dérangeants car ils arrivent tous les jours et encombrent votre boîte de réception.

⇨ Les applications trompeuses

Ces applications vous informent de manière trompeuse sur le statut de sécurité de votre ordinateur, vous affirment que celui-ci est infecté par un malware et que vous devez télécharger un outil pour supprimer la menace. Lorsque vous téléchargez l'outil, il vous signale de soi-disant menaces dans votre ordinateur. Pour les éliminer, vous devez acheter le produit pour lequel des données personnelles sont demandées, comme votre numéro de carte de crédit, etc., ce qui représente un danger.

⇨ Les cookies de suivi

Un cookie est un fichier texte brut qui est stocké sur votre ordinateur dans un dossier Cookies et qui stocke des données relatives à votre session de navigation. Les cookies sont utilisés par de nombreux sites web pour suivre les informations relatives aux visiteurs. Un cookie de suivi mémorise toutes vos informations de navigation et celles-ci sont utilisées par les sociétés et les pirates informatiques pour tout savoir de vos données personnelles, telles que vos coordonnées bancaires, votre numéro de carte de crédit, etc., ce qui représente un danger. Il est possible de les supprimer en **effaçant les données de navigation** ou en utilisant un logiciel qui s'en chargera, du type **Ccleaner.**

Lors de l'atelier « Paramétrage et Sécurité », vous apprenez comment sécuriser votre ordinateur avec un Antivirus et un Antispyware. Utiliser Windows Defender ainsi que le pare-feu de Windows. Mais également à sécuriser votre boîte mail.