Projet 1 – Un peu plus de sécurité, on n'n a jamais assez !

1 – Introduction à la sécurité sur Internet

1/Trois articles parlent de sécurité sur internet.

- Article 1 = F-Secure --Articles et conseils utiles sur la sécurité en ligne
- Article 2 =La Jaune et la Rouge--liberté sur l'Internet
- Article 3 = Cairn.info --L'informatique et sa sécurité

2- Créer des mots de passe forts

1/Utilisation d'un gestionnaire de mot de passe nommé LastPass : il propose un niveau de sécurité optimal.

- On accède au site de LastPass
- On va créer un compte et remplir le formulaire. Et puis on choisi un mot de passe maître avec un niveau de sécurité très élevé.
- Après la création du compte, on se trouve dans la page de validation proposant la téléchargement de l'extension.
- On s'y connecte dès que l'extension est installé.
- Lors de la connexion , on peut enregistrer le mot de passe grâce LastPass.
- On y peut aussi ajouter des comptes manuellement en accédant au coffre-fort, espace de stockage de tous les mots de passe. Il faut juste cliquer sur l'icône de l'extension et sur « Ouvrir mon coffre-fort ».

✂L'abonnement gratuit (freemium) permet de faire des tâches principales. Il permet de synchroniser le compte LastPass sur tous les supports utilisés.

6- Fonctinnalit2 de sécurité de votre navigateur

1/Les sites web qui semblent être malveillants :

- www.morvel.com : Dérivé de www.marvel.com , le site web officiel de l'univers Marvel
- www.docomics.com: Dérivé de www.doccomics.com , le site web officiel de l'univers DC Comics
- www.fessebook.com: Dérivé de www.facebook.com , le plus grand réseau social du monde
- www.instagam.com: Dérivé de www.instagram.com , un autre réseau social très utilisé

2/Vérification si les navigateurs soient utilisés (Chrome/Firefox)

- Pour Chrome :
  -On ouvre le menu du navigateur et accède aux « Paramètr »
  -On clique sur la rubrique « A propose de Chrome »
  -Si le message « Chrome à jour » est constaté, c'est OK
- Pour Firefox
  -On ouvre le menu du navigateur et accède aux « Paramètres »
  -Dans la rubrique « Général », on fait défiler jusqu'à voir la section « Mise à jour de Firefox (astuce : on peut également saisir dans la barre de recherche « mise à jour » pour tomber directement dessus)

✂Firefox affiche une personnalisation des paramètres un peu plus poussée.

4- . Éviter le spam et le phishing

1/Exercice4–Spam et Phishing

On peut aussi consulter des ressources annexes pour s'exercer.

5- Comment éviter les logiciels malveillants

3/Pour chaque site on devra préciser l'indicateur de sécurité et le rapport d'analyse de l'outil Google.

- Site n°1
  -Indicateur de sécurité
    - HTTPS

  -Analyse Google

    - Aucun contenu suspect
- Site n°3
  -Indicateur de sécurité
    - Not secure

  -Analyse Google
    - Aucun contenu suspect
- Site n°3
  -Indicateur de sécurité
    - Not secure

  -Analyse Google

    - On vérifie un URL en particulier.

6- Achats en ligne sécurisés

1/Création d'un registre des achats pour que les informations relatives aux achats en lignes.

Deux possibilités qui sont offertes pour organiser le registre :

1 .On va créer un dossier sur la messagerie électronique

2. On va créer un dossier sur l'espace de stockage personnel

✂La plus pratique à utiliser et facile à mettre en place est la première.

- On accède à la messagerie électronique
- On trouve sur la gauche les libellés initialement prévus sur la page d'accueil du messagerie
- On clique sur « Plus » et va tout en bas des libellés . On clique sur « Créer un libellé » et le nommer « ACHATS » pour créer un libellé.
- On effectue un clic sur le bouton « Créer » pour valider l'opération
- En effectuant un clic sur « Gérer les libellés ».

7- Comprendre le suivi du navigateur

On parle également de suivi du navigateur , de suivi numérique, de suivi des données ou de suivi web. En termes plus simples, les suivi sur Internet correspond à la façon dont les sites web étudient notre comportement lorsque nous les visitons.

8- Principes de base de la confidentialité des médias sociaux

1/Le réglage des paramètres de confidentialité pour Facebook

- On se connecte sur le compte Facebook
- On clique sur le « Paramètres et confidentialité » dès qu'on est sur la page d'accueil
- Ce sont les onglets « Confidentialité » et « Publications publiques » qui sont intèressants.
- La première rubrique résume les grandes lignes de la confidentialité sur Facebook
- Pour retourner dans les paramètres généraux , on effectue un clic sur la croix en haut à gauche.
- Dans les paramètres Facebook on a aussi un onglet « Cookies ».

✂Sur les autres médias sociaux , on retrouvera sensiblement le même type de paramétrage.

9- Que faire si votre ordinateur est infecté par un virus

1/Un exercice pour la vérification de la sécurité d'un site web

*10 étapes :

1. Recherchez le sceau de confiance du site web
La première étape pour vérifier la sécurité d'un site web consiste à rechercher le sceau Website Trust. Ce sceau est un symbole qui indique que la sécurité d'un site web a été vérifiée par une organisation tierce.
Le sceau affiche le nom et l'adresse électronique de l'organisation qui l'a délivré, ainsi que l'URL de son site web et ses coordonnées. Certains sceaux affichent également un nombre indiquant combien d'autres sites web ont été vérifiés avant le vôtre.
La meilleure façon de déterminer si un site web a été vérifié est de consulter sa page d'accueil. Le sceau est généralement affiché sur cette page ou dans le pied de page si le site a été vérifié.
2. Examiner la conception et la fonctionnalité du site web
Pour évaluer l'authenticité et la sécurité d'un site web, il est essentiel d'examiner de près sa conception et ses fonctionnalités, car elles peuvent fournir des indications précieuses sur le caractère authentique ou potentiellement trompeur du site, surtout si l'on tient compte de l'attention portée aux détails lors de la création d'un site web. Si le site ne semble pas professionnel, cela peut indiquer qu'il n'est pas sécurisé. Certains sites frauduleux utilisent les modèles d'un constructeur de site web pour tenter de paraître plus professionnels, il faut donc également rechercher les incohérences dans la marque.
Par exemple, si le site Web comporte de nombreuses fenêtres contextuelles ou demande des informations personnelles sans en expliquer la raison, il peut être suspect.
3. Vérifier l'utilisation du protocole HTTPS
Un site web utilisant le protocole HTTPS aura "https" dans sa barre d'adresse au lieu de "HTTP", ce qui indique qu'il utilise le protocole de transfert hypertexte sécurisé (HTTPS).
Ce protocole crypte toutes les données transmises entre les utilisateurs et les serveurs afin que des tiers ne puissent pas les lire ou les intercepter. Toutes les informations sensibles, telles que les données personnelles et les mots de passe, restent sécurisées tout au long de la transmission.
4. Utiliser des vérificateurs de certificats SSL
Plusieurs vérificateurs de certificats SSL sont disponibles en ligne et permettent aux utilisateurs d'entrer l'URL de n'importe quel site web et de savoir si un certificat SSL y est installé.

Ces outils peuvent être très utiles car ils permettent aux utilisateurs de déterminer rapidement si leurs sites web préférés sont sécurisés. Utilisez ces services chaque fois que possible pour savoir si vos sites web préférés sont suffisamment sûrs pour faire des achats en ligne.

5. Vérifier les sceaux de confiance affichés sur le site web

De nombreux sites web affichent des sceaux de confiance sur leur site pour montrer qu'ils respectent les normes industrielles et les meilleures pratiques en matière de sécurité.

Ces sceaux donnent confiance aux utilisateurs dans leurs transactions en ligne, car ils savent que le site prend la sécurité au sérieux et ne compromettra pas leurs données. Les sceaux de confiance ne sont que l'une des caractéristiques essentielles dont un site a besoin pour inspirer confiance aux visiteurs, au même titre que les informations de contact complètes de l'entreprise en question. Si le site permet à ses clients d'entrer en contact avec lui au moyen d'un logiciel VoIP, il s'agit là d'un autre indicateur de fiabilité à surveiller.

6. Consulter la politique de confidentialité du site web

L'examen de la politique de confidentialité d'un site web est une étape importante pour déterminer s'il est sûr. La politique de confidentialité doit indiquer clairement quelles informations sont collectées, comment elles sont utilisées et qui y a accès.

Si vous ne voyez rien concernant la collecte de données, vous pouvez supposer qu'ils ne collectent aucune information vous concernant (sauf indication contraire).

Si vous voyez quelque chose à propos de la collecte de données, jetez un coup d'œil à leur politique de conservation des données.

Assurez-vous qu'ils ne conservent pas de données inutiles (comme des adresses IP ou des cookies) sur leurs serveurs après la fin de votre interaction, car elles pourraient être utilisées contre vous plus tard.

7. Vérifier la réputation d'un site web avec les services de réputation

Les services de réputation sont un excellent moyen de vérifier la légitimité d'un site web.

Vous pouvez les utiliser pour vérifier s'il y a eu des plaintes ou des rapports concernant des escroqueries par hameçonnage, un service clientèle médiocre ou d'autres problèmes signalés par d'autres utilisateurs.

C'est particulièrement important lorsque vous recherchez un détaillant en ligne ou une institution financière, car cela peut vous aider à éviter les sites compromis par des pirates ou des escrocs.

8. Analyser la sécurité des sites web avec des scanners de sécurité

Les scanners de sécurité sont un autre excellent moyen de vérifier la sécurité des sites web. Ils vous permettent d'analyser les pages à la recherche de logiciels malveillants et de tentatives d'hameçonnage avant de poursuivre vos recherches.

Ces outils analysent également les sites web à la recherche de vulnérabilités et d'autres problèmes susceptibles d'entraîner des failles de sécurité à l'avenir.

9. S'assurer que des méthodes de paiement sécurisées sont disponibles

Avant d'effectuer des achats en ligne, assurez-vous que votre fournisseur de moyens de paiement accepte les transactions sécurisées sur le site.

Certains sites web n'acceptent que les cartes de crédit. D'autres n'acceptent que les paiements par PayPal, tandis que d'autres encore offrent les deux options et plus encore.

10. Effectuer un test de vulnérabilité du site web

Si vous souhaitez en savoir plus sur le degré de sécurité d'un site web, envisagez de le soumettre à des tests de vulnérabilité.

De nombreux types de tests peuvent être effectués, mais un exemple serait d'exécuter un outil de balayage automatisé sur le site web pour voir s'il y a des vulnérabilités connues.

Cela permettra d'obtenir des informations précieuses sur les domaines à améliorer, afin de les traiter avant que les pirates ne les exploitent à des fins malveillantes.

Exploiter DMARC pour la

2/ Exercice pour l’installation et utilisation d’un antivirus+ antimalware.

I. Effectuer un scan antivirus ou anti-malware

A. Accéder à la fonctionnalité Scan virus / Malware de votre hébergement

Pour effectuer un scan d'anti-virus et d'anti-malware sur votre hébergement, suivez les étapes suivantes :

Etape 1 : connexion au panel client LWS.

Vous devez en premier lieu vous connecter à votre espace client LWS afin d'accéder à la gestion de votre hébergement. Cette documentation vous aide à vous y connecter.

Etape 2 : Accéder à la gestion de l'antivirus et anti-malware de votre hébergement

Pour ce faire, dans un premier temps, sélectionnez l'hébergement qui vous intéresse dans la liste des produits de votre compte

Une fois dans la gestion de votre hébergement, repérez la rubrique "Sécurité".
Cliquez ensuite sur "Scan Virus / Malware"

B. Lancer un scan manuel

Lorsque vous accédez à la fonctionnalité "Scan Virus / Malware", l'onglet "scan" ainsi que son contenu est automatiquement affiché. Cette page vous permet de lancer manuellement un Scan Antivirus ou un Scan d'intégrité Wordpress directement

Le scan manuel antivirus

Un scan antivirus d'hébergement web est une procédure effectuée pour vérifier la présence de logiciels malveillants sur les sites web hébergés. Il s'agit d'un processus qui examine les fichiers et les scripts exécutés sur le serveur à la recherche de codes ou de comportements suspects.

L'objectif principal d'un scan antivirus d'hébergement web est de **détecter et de supprimer les logiciels malveillants** tels que les virus, les chevaux de Troie, les scripts malveillants, les programmes indésirables, les backdoors et autres formes de logiciels nuisibles. Les scans antivirus sont essentiels pour **garantir la sécurité des sites web hébergés**, protéger les données des utilisateurs et prévenir les attaques potentielles.

Lors d'un scan antivirus d'hébergement web, les fichiers et les répertoires de chaque site web sont analysés à la recherche de **signatures connues de logiciels malveillants**.

Si un logiciel malveillant est détecté, LWS prend des mesures pour **mettre en quarantaine** les fichiers infectés afin de protéger les autres sites hébergés sur le serveur. **Vous êtes alors informé des résultats du scan** et des mesures prises pour résoudre le problème.

Le scan Wordpress.Un scan d'intégrité WordPress est un processus qui vérifie l'intégrité des fichiers de votre installation WordPress. Il s'agit essentiellement d'une vérification de la structure et de l'intégrité des fichiers principaux de WordPress, tels que les fichiers du cœur de WordPress, les thèmes et les plugins installés.

L'objectif principal d'un scan d'intégrité WordPress est de détecter les modifications indésirables ou les fichiers corrompus .