GASSENDI

mardi 18 octobre 2022

Excursions en informatique du mercredi an 3 : séquence N°03 ;Sécurité

Élaboration	
18 octobre 2022	
Thierry Le Cocq	GASSENDI
Animateur	
Administration informatique	
Nom du fichier	Excurions_2_apprenant_cours_3_V0.1.odt

SOMMAIRE

Table des matières

A) Cours....5
1) Exercice 1....5
2) Exercice 2....5
3) Exercice 3....6
4) Exercice 4....6
5) Exercice 5....6
6) Les conseils....6
7) Encore des conseils....7
8) Vous êtes attaqués....7
9) Des symptômes....7
10) Des solutions : Le problème est sur votre PC :....8
11) Encore des solutions : le problème est sur Internet....8

Objectif général

Anticiper et réagir à la menace, rétablir un fonctionnement normal.

Objectifs de la séquence

Vous serez en mesure :

- ✔ De sauvegarder vos fichiers personnels avant l'attaque, de préparer le rétablissement de la situation
- ✔ De protéger votre PC.
- ✔ D'identifier une attaque discrète.
- ✔ De réagir à une attaque.
- ✔ De rétablir votre PC après une attaque.
- ✔ De trouver une solution si piratage d'un compte.

A) COURS

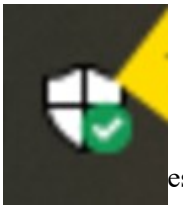
1) Exercice 1

- Insérer votre clé USB.
- Afficher deux fenêtres de l'explorateur de fichiers.
- D'un côté le dossier Bureau de l'autre, votre clé USB
- Glisser le dossier de votre clé USB. / Excursions_mercredi_An_3_Cours_02_apprenants…. vers Bureau
- Créer un dossier : Excursions_du_ mercredi dans le dossier Documents du PC (si ce n'est pas déjà fait).
- Copier le dossier : Excursions_mercredi_An_3_Cours_03_apprenants_... depuis votre clé USB vers le dossier PC \ Documents \ Excursions_mercredi . (si ce n'est pas déjà fait)
- Copier le dossier : Excursions_mercredi_An_3_Cours_02_apprenants...depuis votre bureau vers le dossier : PC \ Documents \ Excursions_mercredi .

2) Exercice 2

- Identifier vos 3 supports de sauvegarde
- Installer FreeFileSync depuis le dossier exercices fichier FreeFileSync_11.27_Windows_Setup.exe
- Connecter votre disque dur externe, voire une clé USB (pas géniale comme idée)
- Ajouter les dossiers à sauvegarder.
- Créer les dossiers de sauvegarde sur votre disque dur externe (ou clé USB)
- Cliquer sur le bouton Comparer. (les fichiers à synchroniser sont alors affichés).
- Cliquer sur le bouton Synchroniser.
- Par la suite seuls les changements du dossier téléchargements seront pris en compte (suppression, modifications, ajouts, ...)

3) Exercice 3

- Aller dans les paramètres de votre PC
- Vérifier la fenêtre Windows Update.
- Mettre à jour le cas échéant
- Vérifier que l'icône sécurité de Windows 10  est visible et au vert sinon :
  - Déplacer l'icône en partie visible de la zone de notifications
  - cliquer sur l'icône et corriger les anomalies

4) Exercice 4

- Le site Avira propose un outil qui se met sur une clé USB (https://support.avira.com/hc/en-us/articles/360007776058-Creating-and-using-Avira-Rescue-System) Cet Outil nécessite de savoir installer une image ISO sur clé USB en utilisant le logiciel Rufus (ce logiciel est dans le dossier exercices de ce cours.
- Rien ne vous empêche de télécharger l'outil Avira et de créer une image sur une clé USB.

5) Exercice 5

- Si vous tentiez de mettre Linux sur un vieux PC ?

6) Les conseils

- Restez prudent lors :
  - De la navigation sur Internet.
  - Du traitement des mails.
  - Des logiciels piratés.
  - Des sites de partages de vidéos, musiques,images, logiciels illégaux.
  - De l'utilisation des réseaux wifi gratuits.
- Pas de bol :
  - Attaque sur des serveurs (d'entreprises, commerces, banque).
  - Piratages de votre réseau Wi-Fi
- Faites :

- Utiliser un PC dédié sous Linux pour les opérations délicates (achats, ...)
- Naviguer en privée sur une machine qui ne vous appartient pas.
- Utiliser un navigateur Internet à jour.
- Des mots de passe spécifiques à chaque site ou de l'argent ou des valeurs sont potentiellement exposés.
- Si un mail provient de votre banque, fournisseur => aller directement sur le site en passant par un favori éprouvé de votre banque, fournisseur..

7) Encore des conseils

- Utiliser un PC dédié sous Linux pour les opérations délicates (achats, ...)
- Naviguer en privée sur une machine qui ne vous appartient pas.
- Utiliser un navigateur Internet à jour.
- Des mots de passe spécifiques à chaque site ou de l'argent ou des valeurs sont potentiellement exposés.
- Si un mail provient de votre banque, fournisseur => aller directement sur le site en passant par un favori éprouvé de votre banque, fournisseur..

8) Vous êtes attaqués

- Ne payez pas !!!
- Touches F11, echapp.
- Photographier votre écran.
- Éteignez votre ordinateur réfléchir et éventuellement demander conseil (on est là aussi pour ça).
- Utiliser un autre ordinateur pour rechercher des infos en fonction du message.

9) Des symptômes

- Une fenêtre avec un téléphone à appeler : F11 , echap, éteindre le PC
- Beaucoup de pop-up
- Plantages fréquents
- Ordinateur lent
- Votre mot de passe change soudainement
- Votre page d'accueil est différente
- Courriels en masse envoyés en votre nom

10) Des solutions : Le problème est sur votre PC :

- Faite un scan avec votre antivirus
- Télécharger et utiliser Adwcleaner de la société MalwaresBytes
- Lancer votre clé USB bootable de secours Avira Rescue System.
- Réinstaller Windows 10 et vos logiciels et vos fichiers.

11) Encore des solutions : le problème est sur Internet.

- https://monitor.firefox.com/
- Changer vos mots de passe (sur Internet) identiques à celui qui a été piraté depuis un PC sain (pourquoi pas depuis votre vieux PC sous Linux).
- https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/que-faire-en-cas-de-piratage-de-boite-mail
- https://www.cybermalveillance.gouv.fr/diagnostic/accueil