Leçon 5 – Protection des données et confidentialité

Équipe Pédagogique Réseau Informatique@ UVCI
2018

Juin 2018
Version 1.0

Table des matières

Objectifs

A la fin de cette leçon, vous serez capable de :

- Présenter l'intérêt de protéger vos périphériques et données personnelles
- Présenter l'intérêt de la sécurisation des données.

Introduction

Cette leçon s'intéresse à la protection des périphériques et données personnels. Elle présente des conseils et techniques pour la protection des périphériques, la sécurisation des données sur le réseau local et celles stockées en ligne.

Protection des périphériques informatiques

Objectifs

Présenter l'intérêt de protéger vos périphériques et données personnelles

1. Étapes pour protéger les périphériques

Les périphériques informatiques (smartphones, tablettes, PC ...) stockent les données et représentent le portail de la vie en ligne. Voici une liste des étapes à suivre pour protéger les périphériques informatiques d'une intrusion .

1.1. Activer toujours le pare-feu

Que ce soit un pare-feu logiciel ou un pare-feu matériel sur un routeur, il doit être activé et mis à jour pour empêcher l'accès des pirates à vos données personnelles ou d'entreprise.

1.2. Utiliser un antivirus et un anti-logiciel espion

Les programmes malveillants (virus, chevaux de Troie, vers, rançongiciels, logiciels espions) s'installent sans autorisation sur vos périphériques informatiques, afin d'obtenir l'accès à votre ordinateur et à vos données.

Les virus peuvent détruire vos données, ralentir votre ordinateur ou prendre son contrôle (prendre le contrôle et diffuser des pourriels à partir de votre compte).

Le logiciel espion peut surveiller vos activités en ligne, collecter vos informations personnelles ou produire des publicités contextuelles indésirables sur votre navigateur Web lorsque vous êtes en ligne.

1.2.1. Les bonnes règles

(1) Ne Télécharger que les logiciels venant de sites Web sécurisés afin d'éviter si possible l'intrusion du logiciel espion.

(2) Installer un logiciel antivirus et le maintenir à jour pour protéger votre ordinateur des derniers programmes malveillants. Le logiciel antivirus est conçu pour analyser votre ordinateur et les e-mails reçus afin de détecter les virus et de les supprimer. Parfois, le logiciel antivirus inclut également un anti-logiciel espion.

1.2.2. Gérez votre système d'exploitation et votre navigateur Web

Les pirates s'efforcent toujours de tirer profit des vulnérabilités des systèmes d'exploitation et des navigateurs Web. Pour protéger votre ordinateur et vos données :

(1) configurez les paramètres de sécurité de votre ordinateur et de votre navigateur Web à un niveau

moyen ou supérieur ;

(2) Mettez à jour le système d'exploitation de votre ordinateur, notamment vos navigateurs Web et téléchargez et installez régulièrement les derniers correctifs de logiciel et les mises à jour de sécurité des fournisseurs.

1.3. Protéger tous vos périphériques

(1)- Les périphériques informatiques (PC, ordinateurs portables, tablettes, smartphones) doivent être protégés par un mot de passe pour empêcher tout accès non autorisé.

(2)- Les informations stockées doivent être chiffrées, surtout les données sensibles et confidentielles.

(3)- Pour les terminaux mobiles, ne stockez que les informations nécessaires. Au cas où ces périphériques seraient volés ou perdus lorsque vous sortez ; si l'un de vos périphériques est compromis, les cybercriminels peuvent avoir accès à toutes vos données par l'intermédiaire de votre fournisseur de service en nuage, comme iCloud ou Google Drive.

(4)- Utiliser une connexion réseau isolée (différente du réseau local) pour les appareils connectés à l'IoT (Internet of Things ou Internet des Objets en français) et de la partager uniquement avec d'autres appareils connectés à l'IoT.

2. Utiliser les réseaux sans fil en toute sécurité

Les réseaux sans fil permettent aux périphériques à accès Wi-Fi, comme les ordinateurs portables et les tablettes, de se connecter au réseau grâce à l'identificateur de réseau SSID (Secure Set Identifier).

2.1. Les mesures de protection

(1)- Pour empêcher l'accès des intrus à votre réseau sans fil domestique, l'identificateur SSID préfiguré et le mot de passe par défaut de l'interface administrative du navigateur Web doivent être changés. Les pirates connaissent ce type d'informations d'accès par défaut.

(2)- De plus, vous devez crypter votre communication sans fil en activant la sécurité sans fil et la fonctionnalité de chiffrement WPA2 du routeur sans fil.

(3)- Le routeur sans fil peut également être configuré pour ne pas diffuser l'identificateur SSID, ajoutant ainsi une barrière supplémentaire à la détection du réseau, sans pour autant être une sécurité adéquate pour le réseau sans fil.

(4)- Il est recommandé de ne pas accéder ou envoyer d'informations personnelles sensibles sur un réseau sans fil public (zone d'accès Wi-Fi permettant d'accéder à vos informations en ligne et de naviguer sur Internet lorsqu'on sort). Vérifiez si votre ordinateur est configuré pour le partage de fichiers et de médias et s'il nécessite une authentification des utilisateurs avec un chiffrement.

(5)- Pour empêcher l'interception de vos informations par un tiers (ou « écoute illicite ») en cas d'utilisation d'un réseau sans fil public, utilisez des tunnels et services VPN chiffrés. Le service VPN vous fournit un accès à Internet sécurisé, avec une connexion chiffrée entre votre ordinateur et le serveur VPN du fournisseur de service VPN. Grâce au tunnel VPN chiffré, même si la transmission des données est interceptée, elle est non déchiffrable.

(6)- Désactivez le Bluetooth lorsque vous ne l'utilisez pas car cette technologie peut pour éviter peut être exploitée par les pirates pour une écoute illicite de certains périphériques, pour configurer des contrôles d'accès à distance, pour distribuer des programmes malveillants et pour décharger les batteries.

3. Utiliser des mots de passe uniques pour chaque compte en ligne

3.1. Mots de passe fiables

Utiliser des mots de passe fiables et uniques pour éviter que vous et vos données soient vulnérables aux cybercriminels. Si les cybercriminels ont eu votre mot de passe par hameçonnage par exemple, ils essaieront d'accéder à vos autres comptes en ligne pour voler ou supprimer toutes vos données, ou

décideront d'emprunter votre identité.

3.2. Gestionnaire de mots de passe

La solution pour éviter de réutiliser les mots de passe ou d'utiliser des mots de passe trop simples lorsqu'on utilise beaucoup de comptes en ligne consiste à utiliser un gestionnaire de mots de passe (stocke et chiffre tous les mots de passe uniques et complexes). Le gestionnaire peut vous permettre de vous connecter automatiquement à vos comptes en ligne. Vous devez seulement vous rappeler de votre mot de passe principal pour accéder au gestionnaire de mots de passe et pour gérer tous vos comptes et vos mots de passe.

3.3. Conseils pour choisir un bon mot de passe

- N'utilisez pas des mots et des noms du dictionnaire, peu importe la langue.
- N'utilisez pas les fautes d'orthographe des mots du dictionnaire.
- N'utilisez pas des noms d'ordinateur ou des noms de compte.
- Si possible, utilisez des caractères spéciaux, comme ! @ # $ % ^ & * ( ).
- Utilisez un mot de passe comptant 10 caractères ou plus.

4. Utilisez une phrase de passe et non un mot de passe

Pour empêcher un accès physique non autorisé à vos périphériques informatiques, utilisez des phrases de passe et non des mots de passe. Les phrases de passe plus longues sont moins vulnérables aux attaques de force brute ou de dictionnaire.

4.1. Conseils pour choisir une bonne phrase de passe

- Choisissez une phrase significative.
- Ajoutez des caractères spéciaux, comme ! @ # $ % ^ & * ( ).
- Plus c'est long, mieux c'est.
- Évitez les phrases courantes ou célèbres, par exemple, des textes d'une chanson populaire.

Remarque

Même si l'accès à vos ordinateurs et à vos périphériques réseau sont sécurisés, il est également important de protéger et de sécuriser vos données.

5. Exercice

[Solution n°1 p 12]

Exercice : Question 1

Quel mot de passe est plus sûr dans la liste ci-dessous

- ◯ A) CoursDeSecurtite
- ◯ B) #C@ursDeSecurite2018#
- ◯ C) coursdesecurite

6. Exercice : Activité 2

Importance du chiffrement des données ; en plus des mesures de protection des périphériques

Question

Réfléchir sur l'importance de chiffrer les données, en plus des dispositions prises pour protéger les périphériques ?

Maintenance des données

II

Objectifs

Présenter l'intérêt de la sécurisation des données.

1. Chiffrer les données

Définition : Chiffrement

Le chiffrement est un processus de conversion des informations en un format non accessible en lecture pour une partie non autorisée.

Remarque

Seule une personne fiable et autorisée, dotée du code secret ou du mot de passe peut déchiffrer les données et accéder à leur format original. Le chiffrement proprement dit n'empêche pas l'interception des données par un tiers. Le chiffrement ne peut qu'empêcher une personne non autorisée à visionner ou à accéder au contenu.

1.2. Pourquoi chiffrer les données ?

Même si l'on pense ne pas avoir de secrets, ni de choses à cacher, les données doivent être chiffrées car elles sont importantes sous certaines angles.

Si votre ordinateur est infecté par une application malveillante par exemple, elle peut :

- montrer toutes vos photos et tous vos documents à des étrangers
- partager avec vos amis les informations financières stockées sur votre ordinateur
- voler les mots de passe de votre e-mail et de vos comptes au public
- voler des informations potentiellement utiles, comme les numéros de compte, les mots de passe et d'autres documents officiels. Ce type d'informations peut mener à l'usurpation d'identité, à la fraude ou à une demande de rançon. Les cybercriminels peuvent décider de simplement chiffrer vos données pour les rendre inutilisables jusqu'à ce que vous payiez la rançon.

Des programmes sont utilisés pour chiffrer des fichiers, des dossiers et même des disques entiers.

2. Sauvegarder les données

2.1. L'intérêt de sauvegarder

Avoir une sauvegarde permet d'empêcher la perte de données irremplaçables en cas de panne du disque dur, de perte ou vol de l'ordinateur ou du smartphone ou de suppression de la version originale d'un document important.

2.2. Conseils pour bien sauvegarder

Pour bien sauvegarder les données, il faut :

- avoir une mémoire supplémentaire pour vos données,
- copier régulièrement et automatiquement les données dans cette mémoire.

2.3. Exemples de mémoire supplémentaire pour la sauvegarde des fichiers

- réseau domestique (stockage en réseau NAS),
- une mémoire secondaire (disque dur externe, clés USB, CD/DVD),
- ou le cloud (service de stockage du cloud comme Amazon Web Services, AWS).

3. Supprimer définitivement vos données

Un fichier déplacé dans la corbeille et définitivement supprimé par la suite est toujours accessible à partir du système d'exploitation. Toute personne possédant les bons outils de recherche peut encore récupérer le fichier en raison de l'emprunte magnétique sur le disque dur.

Conseils sur la suppression des données

Afin de supprimer les données pour qu'elles ne soient plus récupérables, ces dernières doivent être remplacées par une suite de uns (1) et de zéros (0) avec des outils adéquats.

La seule manière de certifier que les données ou les fichiers ne sont pas récupérables consiste à détruire physiquement le disque dur ou le périphérique de stockage.

Il faudrait supprimer les copies des données stockées en ligne.

Lorsque vous devez supprimer vos données ou vous débarrasser d'un disque dur ou d'un ordinateur, demandez-vous si vous avez protégé les données pour que des personnes malveillantes n'y aient pas accès.

4. Protection de la confidentialité

Authentification à deux facteurs

Outre le nom d'utilisateur et le mot de passe, ou le modèle ou le numéro d'identification personnelle (PIN) utilisés dans certains services en ligne, l'authentification à deux facteurs nécessite un second jeton, comme :

- un objet physique (une carte de crédit, un téléphone ou un porte-clé)
- un balayage biométrique (une empreinte digitale ou palmaire et une reconnaissance vocale ou faciale).

Ne partagez pas trop d'informations sur les réseaux sociaux

Si vous souhaitez maintenir votre confidentialité sur les réseaux sociaux, partagez le moins d'information possible

Plus vous partagez d'informations personnelles en ligne, plus il est facile pour une personne de créer un profil en votre nom pour en tirer profit hors connexion.

Les questions de sécurité (comme quel est le nom de jeune fille de votre mère ? » ou « dans quelle ville êtes-vous né ?) sont supposées sécuriser votre compte contre l'accès d'intrus. Cependant, toute personne souhaitant accéder à vos comptes peut rechercher les réponses sur Internet. Il est mieux de répondre de façon erronée à ces questions, tant que vous pouvez vous rappeler des réponses incorrectes. Si vous avez des difficultés à vous les rappeler, vous pouvez utiliser un gestionnaire de mots de passe pour les gérer à votre place.

Confidentialité de l'e-mail et du navigateur Web

Les messages transmis par e-mail sont transmis en texte brut et également transférées sur plusieurs serveurs lors de l'acheminement vers la destination. Même si vous supprimez vos messages électroniques, ils peuvent être archivés sur les serveurs de messagerie pour une durée déterminée.

Toute personne ayant accès à votre ordinateur ou à votre routeur peut voir les sites Web que vous avez visités grâce à l'historique de navigation Web, au cache et éventuellement aux fichiers journaux. Ce problème peut être minimisé en activant le mode de navigation privée sur le navigateur Web.

Grâce à l'activation du mode de navigation privée du navigateur web :

- les cookies sont désactivés et les fichiers Internet temporaires et l'historique de navigation sont supprimés à la fermeture de la fenêtre ou du programme.
- on peut réduire le risque que des tiers puissent collecter des informations sur votre activité en ligne pour vous inciter à acheter des choses par le biais de publicités ciblées.

En conclusion, il est de votre responsabilité de protéger vos données, votre identité et vos périphériques informatiques. Il suffit de quelques précautions simples pour vous éviter des problèmes dans le futur.

5. Exercice : Activité 1

Le système EFS (Encrypting File System) de Windows permet de chiffrer des données.

Question

Faire des recherches sur son fonctionnement et l'application de ce programme pour le chiffrement de fichiers.

6. Exercice : Activité 2

Les programmes SDelete de Microsoft, Shred de Linux permettent de supprimer définitivement les fichiers.

Question

1) Faire des recherches sur le fonctionnement et l'application de ces programmes.

2) Chercher d'autres programmes rendant ce même service.

7. Exercice : Activité 3

NAS est un système de stockage en réseau.

Question

Faire des recherches sur le fonctionnement du stockage en réseau NAS.

8. Exercice : Activité 4

Le cloud offre des services de stockage de données.

Question

Faire des recherches sur le fonctionnement des services de stockage offert par le cloud, leurs avantages et inconvénients.

9. Exercice : Activité 5

Le mode de navigation privée permet de minimiser l'accès aux sites web déjà visités. Les navigateurs web ont leur propre dénomination du mode de navigation privée.

Question

Faire des recherches sur l'activation du mode de navigation privée des navigateurs suivants :

- Microsoft Internet Explorer
- Google Chrome
- Mozilla Firefox
- Safari

Solutions des exercices

> Solution n°1

Exercice p. 7

Question 1

- ○ A) CoursDeSecurtite
- ◉ B) #C@ursDeSecurite2018#
- ○ C) coursdesecurite

Bibliographie

1. Stéphane Lohier, Dominique Présent ; Réseaux et transmissions, 6è édition, DUNOD 2016

2. Danièle Dromard, Dominique Seret ; Architecture des réseaux, collection Synthex, 2009 Pearson Education France, ISBN : 978-2-7440-7385-4