Cybersécurité
cours de base

Organisation des cours « Sécurité »(1/4)

- Introduction au cours et organisation générale
- Cours de base :1ere partie :
  - Liste des menaces
  - Les virus/les chevaux de Troie/les vers
  - Généralités sur les mesures préventives,
- Cours de base :deuxième partie
  - Les adwares/les spams/les spywares
  - Les malwares sur téléphone
  - Le chantage à la webcam
  - Le phishing/les ransomwares
  - Le piratage de messagerie
- Cours de base :troisième partie
  - Les actions en cas d'infection

Organisation des cours « Sécurité »(2/4)

- Protections détaillées (appelées dans le cours de base)
  - Cours 1 : Antivirus et firewall (PC et téléphones)
    - Principe de fonctionnement
    - Différences payants/gratuits
    - Comment vérifier la protection de votre ordinateur
    - Désinstallations/installations
    - Avast, Windows defender, utilisation,
    - Gérer le pare feu Windows 10
    - Antivirus sur tablette et téléphone
  - Cours 2 :
    - 2-A Mots de passe
    - 2-B Sauvegardes
  - Cours 3: Mises à jour
    - Windows 10 : installations des mises à jour/suppression d'une mise à jour
    - Mises à jours des logiciels
    - Mises à jour des logiciels sur tablettes et téléphones

Organisation des cours « Sécurité »(3/4)

- Cours 4 : antimalwares (PC et téléphones)
  - Installation/utilisations/mise à jour
  - adwcleaner/malwarebytes
  - Extensions de chrome
    - » Wot
    - » Ublock
- Cours 5 : Application du cours à l'utilisation d'internet (exercices)
  - Vérifier l'état de protection du PC
  - Surfer sur internet
  - Télécharger
  - Se protéger de la publicité
  - Protéger sa messagerie GMAIL
  - Se protéger en utilisant un réseau social
  - Vérifier la fiabilité d'un site de vente

Organisation des cours « Sécurité »(4/4)

- Cours 6 : Entretien de l'ordinateur
  - Pourquoi faire,
  - Glary utilities,
  - Ccleaner
  - Nettoyage navigateur, historique etc…

Introduction

- Ce cours repose en partie sur le site public

https://www.cybermalveillance.gouv.fr/

Il est conseillé de consulter régulièrement ce site qui fournit beaucoup d'informations sur le thème de la sécurité informatique.

Vous pouvez y obtenir de l'aide en cas d'infection via le menu « assistance »

- Il repose également sur un ensemble de sites d'informations tels que « malekal, 01net, commentçamarche »

Généralités

- Pourquoi les malwares existent-ils?

Face à l'explosion du nombre d'utilisateurs d'internet (4,5 milliards), il est assez facile de gagner beaucoup d'argent en trompant, manipulant, piratant les internautes.

- Les malwares évoluent sans arrêt et leur nombre augmente considérablement chaque année;
- 300 à 500000 malwares nouveaux chaque jour sur internet
- Le nombre d'objets connectés augmente sans arrêt (PC, téléphones, tablettes, mais aussi caméras vidéo, TV et tous les objets de la vie courante.
- Le piratage des bases de données utilisateurs des sites (banques, compagnies aériennes, amazon etc….)
- Il est donc indispensable de se protéger
- Pour se protéger des malwares, il faut connaître les méthodes utilisées pour pirater les ordinateurs, et ainsi pouvoir:
  - être vigilant,
  - appliquer des actions de prévention
  - Savoir comment agir en cas d'infection

Sécurisez votre espace numérique

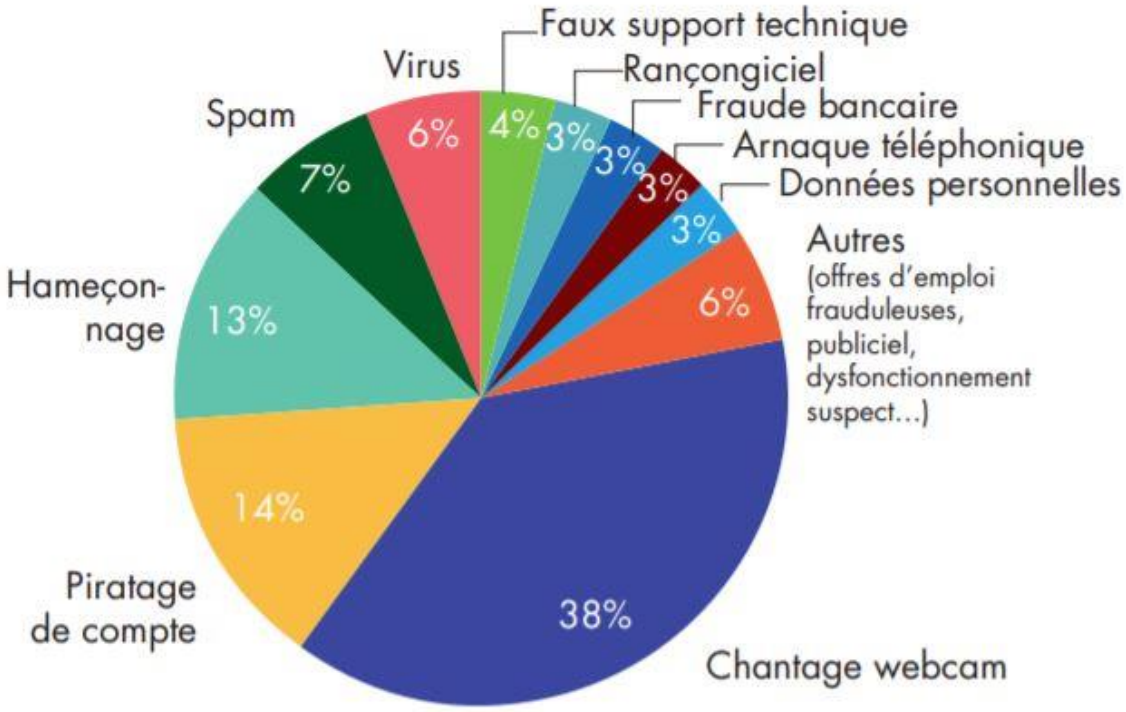
- 3 gestes essentiels:
  - Utiliser un antivirus
  - Sauvegarder vos données
  - Mettre à jour vos logiciels

Les dangers

- Vol d'identité,
- Piratage des données personnelles,
- Prise en otage des fichiers,
- Déferlement de publicités,
- Détournement des ressources du PC
- Etc…

Les dangers pour les particuliers

Statistiques 2019 du site cybermalveillance.gouv.fr;personnes qui demandent de l'aide



Les éléments infectés

- Les logiciels téléchargés,
- Les sites web qui hébergent des codes ou des liens malveillants,
- Les clés et disques durs USB,
- Les fichiers pdf et Office qui contiennent des macros infectées,
- Des mails et les pièces jointes pour vous arracher des informations personnelles

Généralités : ce qui peut être infecté dans votre PC

- Les logiciels de démarrage,
- Les répertoires contenant des programmes,
- Des logiciels du système Windows remplacés par d'autres (infectés) mais avec le même nom
- Les logiciels liés aux navigateurs
- La base de registre,
- Le bios,
- ….

Liste des menaces
(liste non exhaustive)

- Les virus,
- Les chevaux de Troie,
- Les vers,
- Les spywares,
- Les adwares,
- Les spams,
  - Téléphoniques
  - Electroniques
- Le piratage de compte,
- Le chantage à la webcam,
- L'hameçonnage (le phishing),
- Le faux support technique,
- Les rançongiciels (ransomwares)

Les malwares

- Terme générique qui désigne un virus, un ver, un cheval de Troie, un spyware etc…
- A la première exécution, le malware va s'installer dans divers endroits du PC (mémoire, système de démarrage, dossiers windows, registres etc…)
- Le malware peut prendre le nom d'un fichier système et reste ainsi « invisible »,
- Il se lance automatiquement au démarrage du PC
- Les malwares atteignent aussi les tablettes et téléphones,
- Certains malwares désactivent votre antivirus (en forçant un démarrage en mode « sans échec »)

Liste des menaces: virus

- Virus :

Un virus est un programme informatique qui peut se propager à travers les ordinateurs et les réseaux en créant ses propres copies, et cela, généralement à l'insu des utilisateurs.

- Les virus peuvent avoir des effets néfastes :
  - affichage de messages agaçants,
  - subtilisation de données,
  - transfert du contrôle de votre ordinateur à d'autres utilisateurs.

Les actions des virus

- Ralentir la messagerie,
- Subtiliser des données (mot de passe)
- Attaquer d'autres sites web à partir de votre ordinateur,
- Permettre à d'autres utilisateurs de pénétrer dans votre ordinateur,
- Corrompre ou effacer des données
- Désactiver des matériels audio, webcam, disque dur etc…
- Afficher des messages
- Etc…

Les virus: comment infectent-ils?

- Pour infecter un ordinateur, un virus doit « s'exécuter » car c'est un programme.
- Il peut être dissimulé dans un autre programme que l'on installe (jeux, logiciels divers,)
- Il peut être transmis en exploitant des failles du réseaux et des protections du système d'exploitation
- Il peut être contenu dans une pièce jointe d'un e-mail, contenant des photos, des vidéos, des cartes de vœux, dans un site
- C'est au moment de l'exécution du code que le virus devient « actif »
- Une fois installé, il peut s'exécuter automatiquement et se retransmettre
- Les virus se propagent rapidement

Les chevaux de Troie (Trojan)

- *Chevaux de Troie:*

Sont contenus dans des logiciels « légitimes » (logiciels malveillants « déguisés » en logiciels utiles.

Ce sont des programmes qui exécutent des fonctions « cachées » et néfastes

  - Ex : se connecter à des sites web pour saturer le fonctionnement de l'ordi et du réseau
  - Ex : enregistrer et transmettre les frappes du clavier (keylogger)
- Les chevaux de Troie ne se répliquent pas eux-mêmes
- Peuvent permettre à quelqu'un de prendre le contrôle de votre ordinateur à distance (ils ouvrent des portes clandestines) >> Rootkit
- Peuvent accéder à vos fichiers et les modifier
- Ne se propagent pas rapidement
- Peuvent être téléchargés par les virus
- Certains rootkits vont se loger dans le BIOS et résistent ainsi aux antimalwares voire même au formatage du disque dur !

Les vers

- Identiques aux virus mais ne nécessitent pas de support (programme ou document)
- Se dupliquent sans cesse en recréant des répliques exactes d'eux-mêmes (contrairement aux virus)
- Se propagent par transmission entre ordinateurs en exploitant les failles de sécurité;
- Certains utilisent la messagerie pour se transmettre eux-mêmes. L'ordinateur peut être infecté sans que l'e-mail soit ouvert !
- Génèrent beaucoup de trafic internet, occupent beaucoup de place sur les DD. Ils provoquent des ralentissements des communications

Sachez repérer les sites à risques

- Vérifiez l'adresse du site en https et non http (clic sur le cadenas pour vérifier la validité du certificat)
- Attention aux sites dont l'adresse est raccourcie et qui masque l'adresse finale
- Evaluer la fiabilité d'un site avec WOT
- Attention aux fausses alertes de sécurité; fermez le processus avec le gestionnaire de tâches (ctrl+alt+del)
- Des notifications factices propagent des malwares (PC et téléphone)
- Gérer les autorisations
- Paramétrez les réseaux sociaux pour communiquer en sécurité
- Sécuriser les achats en ligne

Protections contre les virus et les vers

- Les antivirus et les pare feux : Voir cours spécifiques
- Accéder au « centre de sécurité Windows » et vérifier les protections : voir cours antivirus
- Faire des sauvegardes : voir cours
- Mettre à jour vos logiciels : voir cours
- Tester les fichiers avant de les ouvrir:
  - En utilisant votre antivirus et votre antimalware,
  - Avec « virustotal » voir cours « actions »
  - En vérifiant la signature du fichier (99% des fichiers infectés n'ont pas de signature)
    - Clic droit sur le fichier/propriétés/signatures numériques)

Fin de la première partie

Cours de base
deuxième partie

Les adwares et PUP (potentially unwanted programs)

- Programmes proposés en option lors de l'installation de logiciels gratuits
- En contrepartie d'un logiciel gratuit, vous recevez une barre d'outils, ou un adware
- Un adware génère des fenêtres de publicités, ou modifie la page de démarrage ou de recherche d'un navigateur web
- On les récupère via :
  - De « faux » logiciels
  - Le résultat du moteur de recherche
  - Des sites de téléchargement (vidéos, musiques, jeux…)
  - Des sites illégaux de streaming
  - Des extensions de navigateur
  - Des fausses mises à jour de logiciels (Java, Adobe…)

Mesures préventives contre les adwares

- Voir cours antivirus
- Extension de navigateur :WOT, Adblock, Ublock origin, Utabs
- Télécharger les logiciels sur les sites d'origine des fournisseurs
- Etre vigilant sur les cases « cochées » lors de l'installation d'un logiciel

Spams téléphoniques

- Les spams téléphoniques

Appels téléphoniques non sollicités à des fins publicitaires, commerciales ou malveillantes:

Incitation à rappeler un numéro de téléphone payant,

Certains appels sont reçus avec le même indicatif régional que le votre (l'escroc utilise une technique qui modifie le n° d'appel pour être plus crédible, imiter un N° d'entreprise)

Les Spams électroniques

- SMS ou MMS, ou courriels
- Incitation à renvoyer un sms à des numéros payants ou tentative d'hameçonnage pour récupérer des informations (données personnelles)

- Comment les reconnaître :
  - Les courriers indésirables
  - L'adresse mail
  - Le langage
  - Les informations demandées

Mesures préventives contre les spams

- Vigilance et ne pas communiquer trop largement votre n° de téléphone; remplissage de formulaires, jeux, tirages au sort, etc…
- Inscription à bloctel
- Utiliser l'annuaire inversé pour savoir à qui appartient le numéro
- Utilisation du filtrage de numéro (possible avec certains opérateurs)
- Se désabonner des comptes que l'on n'utilise plus,
- Ne pas rappeler les numéros (inconnus)laissés sur votre répondeur en votre absence
- Ne pas renvoyer un sms vers un numéro payant
- Ne pas cliquer sur un lien reçu via un sms inconnu

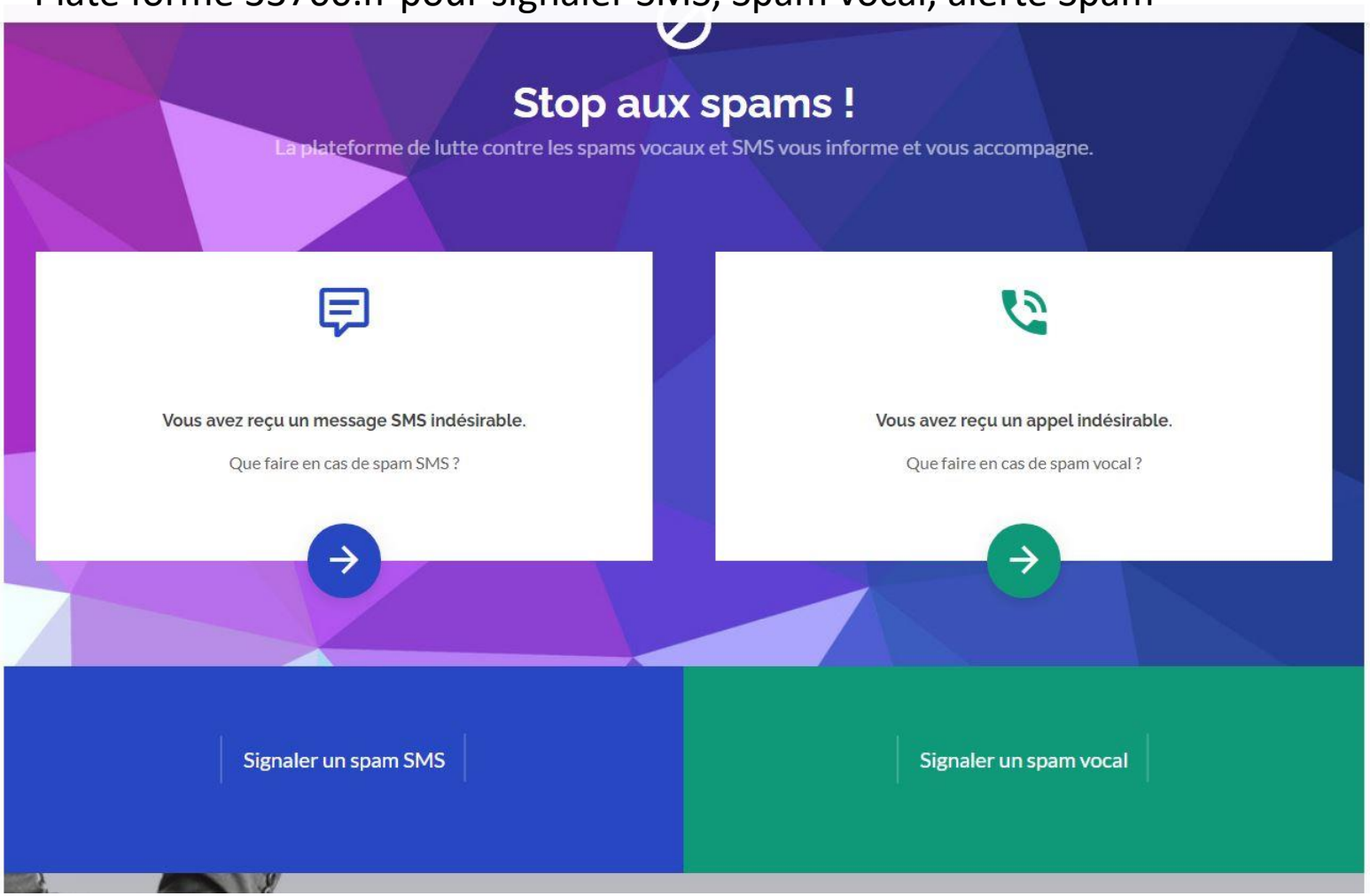
Actions contre les spams (avec le téléphone)

- Spam téléphonique :Bloquer le numéro que vous ne souhaitez plus recevoir : appli téléphone/paramètres/bloquer les numéros
- Signaler les spams téléphoniques à la plateforme (33700), à « signal spam »
- Faire une réclamation à BLOCTEL
- Spam électronique : bloquer le numéro du message :
  appli de messagerie/clic sur le message à bloquer/paramètres/bloquer

Selon les applications utilisées le processus de blocage peut être légèrement différent

Actions contre les spams (avec le téléphone)

Plate forme 33700.fr pour signaler SMS, Spam vocal, alerte Spam



Les malwares sur android

- Les smartphones sont des ordinateurs, ils peuvent donc être infectés comme les PC
- Les malwares Android sont en pleine expansion (plus de 25000 applications contiennent des malwares sur le play store de Google)
- Les menaces sont les mêmes que pour les PC
- Elles pénètrent dans les téléphones lors d'un téléchargement (appli douteuses, liens etc…) ou via votre navigateur
- Elles peuvent être pré installées sur des téléphones à bas prix
- Les utilisateurs ne protègent pas aussi bien leurs téléphones que leurs PC

Signes d'infection sur un téléphone

- Le déluge de popups avec des publicités,
- Une augmentation de l'utilisation des données, d'où une consommation du forfait
- Des frais dus à l'envoi de SMS vers des n° surtaxés
- Une baisse de l'autonomie (batterie très sollicitée)
- Vos contacts qui signalent des appels et des SMS en provenance de votre téléphone
- Un téléphone qui chauffe, car très sollicité
- La présence d'applications que vous n'avez pas téléchargée
- L'activation de connexions wifi ou internet sans votre accord

La prévention des malwares sur Android (suite)

- Eviter de cliquer sur les popups,
- Eviter d'ouvrir les pièces jointes provenant d'e-mails inconnus
- Ne pas cliquer sur les liens suspects des mails ou SMS mêmes s'ils viennent d'un ami
- Ne pas installer des applications méconnues provenant de sources non fiables
- Activer le « Play Protect » du Play Store, (tout message incitant à le désactiver est un piège)
- Maintenir le système d'exploitation, les navigateurs et leurs plug ins à jour (voir cours sur les mises à jour)
- Maintenir les applications à jour,(voir cours sur les mises à jours)

La prévention des malwares sur Android

- Contrôler les autorisations que vous fournissez aux applis lors de leur installation
- Télécharger les applications à partir du Play Store, éviter les autres sources (contrôler les installations d'APK)
- Lire les avis avant de télécharger une application
- Etre prudent avant de donner des autorisations d'accès au logiciel que vous venez d'installer (à vos contacts par exemple)
- Utiliser un antimalware (voir cours sur les antimalwares)
- Faites des sauvegardes (voir cours sauvegardes)

Les spywares (logiciels espions)

Le logiciel espion ou spyware est un logiciel qui permet aux publicitaires de rassembler des informations sur les habitudes des utilisateurs de PC.

- Les logiciels espions ne sont pas des virus
- Ils peuvent s'installer sur votre ordinateur lorsque vous visiter un site, ou lorsque vous installez un logiciel utilitaire
- Ils vous suivent à la trace (mouchards)sur vos visites de sites et vos habitudes et transmettent les informations (vol de données, mots de passe…)
- Ils peuvent changer la page d'accueil de votre navigateur
- Ils ralentissent votre ordinateur,
- Peuvent prendre et transmettre des captures d'écran

Cas particulier de spyware :les cookies

Logiciel chargé sur votre ordinateur lorsque vous visitez un site web.

Le site conserve ainsi des traces de votre visite pour les fois suivante et permet ainsi un chargement plus rapide des pages du site

- Certains cookies sont nécessaires pour la bonne consultation des sites web
- D'autres peuvent parfois menacer la sécurité et la confidentialité:
  - Vous pouvez « désactiver les cookies » dans les paramètres de votre navigateur(mais il peut y avoir un impact sur la consultation des sites)

Le pare feu windows 10

- Le pare feu de windows 10 permet de protéger votre PC des malwares en protégeant les « entrées/sorties »
- Il peut parfois bloquer l'installation d'un logiciel ou l'accès à un site;
- C'est une des causes de l'erreur « nous n'avons pas pu charger la page »
- Si vous êtes sûr de la sécurité du logiciel ou du site, il est possible de désactiver le pare feu temporairement. Voir le cours « antivirus et pare feu »

Le chantage à la webcam

- Vous recevez un message d'un hacker qui prétend :
  - Détenir de vous, des vidéos compromettantes,
- Il écrit avec votre e-mail,
- Il cite un de vos mots de passe pour être crédible

  et Il demande une rançon
- En général c'est une arnaque
- Ne payez pas, conservez les preuves (copies d'écran), déposez plainte, changez le mot de passe concerné
- Masquez votre webcam quand vous ne l'utilisez pas (scotch) ou désactivez la.

Les botnets

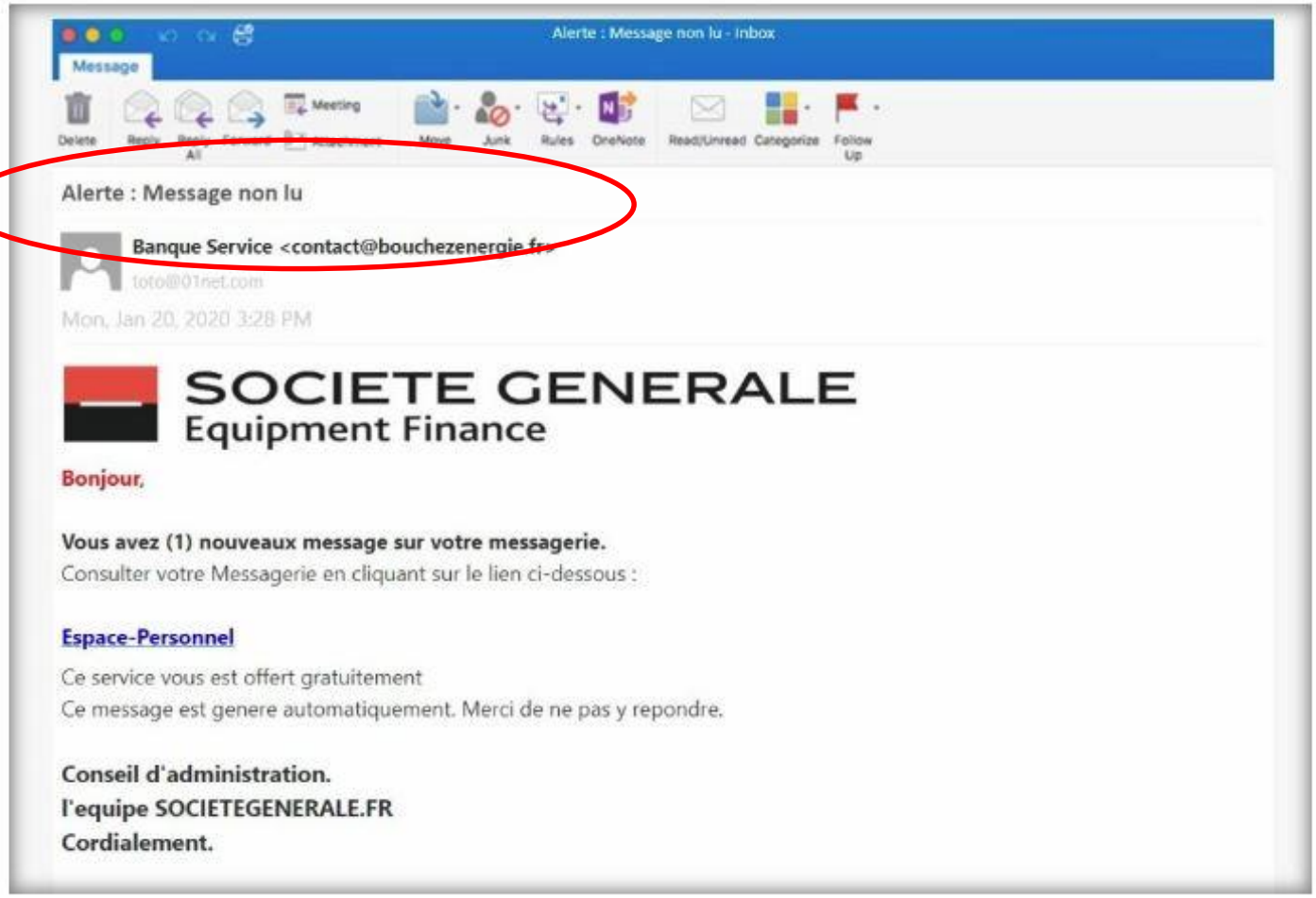
- « robot » et « Network », utilisent une partie de la puissance de l'ordinateur pour participer à des attaques pour rendre indisponible un site web
- Diffusion :mail, téléchargement via un site web infecté
- Principales protections : mettre à jour votre système, vérifier les pièces jointes de mail, antivirus à jour
- En cas de doute vous pouvez contrôler l'activité de votre PC avec le gestionnaire de tâches (ctrl+alt+sup) et localiser le logiciel qui utilise beaucoup de ressources

L'hameçonnage/Phishing

Technique qui consiste à « leurrer » un internaute pour l'inciter à fournir des données personnelles (mot de passe, n° de compte numéro carte bancaire, adresse etc….)

- *Se présentent sous différentes formes imitant de vrais messages:*
  - *Faux messages sms, e-mail,*
  - *Appels téléphoniques, (banque, opérateur, fournisseur d'energie, commerce en ligne, administration (Ameli, Laposte etc….)*

Exemple 1 phishing



Exemple 2 phishing

On joue sur l'espoir de gain

Exemple 3 phishing

On joue sur l'urgence

Mesures préventives contre le hameçonnage

- Ne communiquez jamais d'informations sensibles par messagerie ou téléphone
- Avant de cliquer sur un lien douteux, positionnez le curseur de votre souris sur ce lien (sans cliquer) ce qui affichera alors l'adresse de destination. Si le domaine affiché ne colle pas avec la marque représentée, il y a danger
- Vérifiez l'adresse du site qui s'affiche dans votre navigateur; surtout le nom de domaine:
  - « www.ıkea.com » au lieu de « www.ikea.com »
  - « www.airfrance.com » au lieu de « www.airfrance.com »
- En cas de doute, contactez si possible directement l'organisme concerné
- Utilisez des mots de passes différents et complexes pour chaque site et application
- Si possible, vérifiez les date et heure de dernière connexion à votre compte
- Dans les pièces jointes n'ouvrez que les pdf, jamais les word ni les .zip
- Activez la double authentification pour sécuriser vos accès
- En cas de doute utilisez un service de vérification en ligne comme « isitiphishing.org »
- Site d'entraînement à reconnaître le phishing :Phishing-IQ-Test.com
- Signaler un site de phishing : « phishing initiative » qui bloque l'adresse du site

Les rançongiciels (ransomwares)

Logiciel qui bloque l'accès à l'ordinateur ou à vos fichiers en les chiffrant, et réclame une « rançon » pour vous permettre d'y accéder à nouveau

- Comment être infecté :
  - Pièce jointe d'un e-mail,
  - Clic sur un lien malveillant,
  - Navigation sur un site
  - Intrusion dans votre ordinateur (via une faille du système ou d'un logiciel)
- La sous famille des « cryptologger » chiffre vos données personnelles

Mesures préventives contre les ransomwares

- Tenir à jour vos logiciels
- Tenir à jour l'antivirus et configurer le parefeu
- Ne pas cliquer sur les liens des courriels inconnus (chaînes de messages par exemple)
- Ne pas installer de programmes « douteux » (jeux, logiciels crackés, etc…)
- Eviter les sites peu sûrs (téléchargements illicites, contrefaçons etc…)
- Faire des sauvegardes, (voir cours sauvegardes)
- Gérer vos mots de passe (voir cours mot de passe)
- Eteindre votre Pc si vous ne vous en servez pas

Le faux support technique

Consiste à effrayer la victime, par SMS, téléphone, chat, courriel, ou par l'apparition d'un message qui bloque son ordinateur, lui indiquant un problème technique grave et un risque de perte de ses données ou de l'usage de son équipement

- Un message vous demande de contacter un faux support « officiel » comme apple, microsoft etc… pour payer un dépannage ou acheter un logiciel

Mesures préventives contre les faux support techniques

- Voir les mesures des ransomwares

Piratage des comptes en ligne et des messageries

C'est la prise de contrôle par quelqu'un de malveillant d'un compte (messagerie, réseau social etc…)

- Comment s'en apercevoir : vous ne pouvez plus accéder à vote compte, les amis vous contactent car ils ont reçu des messages de vous « surprenant »,
- Principales conséquences : usurpation d'identité, vol de données bancaires, achats en votre nom, etc…
- Causes principales : vol de votre mot de passe (via les différentes techniques présentées dans ce cours) telles que hameçonnage, mots de passe trop simples ou identiques sur plusieurs comptes, mots de passe fournis sur un mail etc…

Mesures préventives contre le piratage de compte de messagerie

- Voir cours mot de passe et cours messageries
- Appliquer toutes les mesures préventives déjà citées dans ce cours

Se protéger des piratage de comptes en ligne

- C’est le vol des bases de données chez les grands sites (sur leurs serveurs), on compte plusieurs millions de vols chaque années.
- Les informations étant gérées par des tiers, impossible de se protéger du vol
- Se tenir au courant des actualités,
- Changer régulièrement vos mots de passe
- Utiliser la double authentification

Fin de la deuxième partie

Cours de base troisième partie

Actions en cas d’infection

Généralités

- Impossible de traiter tous les scénarios rencontrés lors d'une infection; seuls les cas « basiques » sont traités ci-après.
- Lors d'une infection soit l'antivirus vous avertit, soit il de réagit pas mais le comportement de votre PC est surprenant :
  - ralentissements,
  - Fenêtres intempestifs de publicité
  - Barre d'outils nouvelles,
  - Plantages,
  - Etc…
- Avant toute action il faut
  - Confirmer l'infection,
  - Identifier le type de malware
  - Identifier la source de l'infection (afin que cela ne se reproduise pas)
  - Choisir les actions de désinfection (des outils inapropriés peuvent dégrader la situation)
  - Si nécessaire faire appel à un expert

Actions en cas d'infection
(cas où l'antivirus se déclenche)

- Si vote antivirus vous alerte qu'il vient de détecter une menace, votre PC n'est pas forcément gravement infecté
- >>> pas de panique
- Déconnecter internet,
- Prenez le temps d'analyser la situation

Actions en cas d'infection
(cas où l'antivirus se déclenche)

- Selon la nature de l'infection, les actions a mener peuvent être différentes
- Le cours vous donne quelques éléments pour identifier le type d'infection dont vous êtes victimes
  - Virus,
  - Publicités
  - Piratage de compte,
  - Etc…

Actions en cas d'infection
(cas où l'antivirus ou l'antimalware se déclenche)

- Si l'antivirus a bloqué un site web que vous souhaitiez consulter (ou pas !),
  - Fermez l'onglet concerné,
  - Nettoyez le navigateur (supprimer le cache, historique cookies etc ….)
  - Vérifiez les extensions et supprimer les extensions douteuses et inutiles
- Si l'antivirus a détecté un fichier infecté dans la zone de téléchargement (setup; fichier office, fichier zip etc…),la menace n'est pas active tant que vous n'avez pas encore installé le logiciel; effacez les fichiers et videz la corbeille
- Si l'antivirus a détecté une pièce jointe infectée dans un mail, n'ouvrez pas la pièce jointe, effacez le mail et videz la corbeille
- Par sécurité lancez un scan détaillé avec l'antivirus, lancez malwarebytes, (Chrome dispose aussi d'un outil antimalware)
- Les actions ci-dessus devraient suffire
- Restez attentif au comportement de votre PC, pendant cette période ne pas faire d'opérations « risquées » telles que achats, consultation comptes bancaires etc …

Actions en cas d'infection
(cas où l'antivirus se déclenche)

- Si la menace est déjà répandue dans le PC :
- Analyser les informations données par votre antivirus, pour localiser les différents emplacements et l'identification de la menace
  - Notez le nom des fichiers mis en quarantaine,
  - L'emplacement du virus peut donner une indication sur sa nature.
  - Consultez les forums pour connaître le niveau d'infection avec le nom du malware identifié
  - Utilisez « virustotal » pour confirmer l'infection
  - Effacer les fichiers mis en quarantaine, ou conserver les quelques temps sans les réactiver dans le PC
  - Il se peut que la menace ne soit pas entièrement éradiquée, si vous constatez encore des disfonctionnements
    - Refaite un scan détaillé, voire utilisez un autre antivirus
    - Consulter les forums avec le nom de la menace
    - faites appel a un spécialiste

Confirmation en cas de doute utilisation de « virustotal »

- L'outil « virustotal » est un service gratuit sur internet qui permet d'analyser un fichier ou un site web avec plusieurs antivirus
- Ouvrir le site « virustotal.com »
- Cliquez sur « file(fichier) ou URL (site web) puis « choose file » pour désigner le fichier douteux sur votre disque dur
- Vous obtiendrez un résultat d'analyse fait avec plusieurs antivirus; analyser le résultat.

Actions en cas d'infection (sans déclenchement de l'antivirus)

- Au moindre doute, débrancher le PC ou se déconnecter d'internet
- Ransomware : Ne pas payer la rançon et déposer plainte
- Si possible appliquer une méthode de désinfection :
  - Scan détaillé via votre antivirus et mise en quarantaine du malware si détection, (sinon utiliser « virustotal » si la connexion internet fonctionne, ou un autre antivirus via une clé USB)
  - Adwcleaner, et suppression des malwares détectés
  - Malwarebytes et suppression des malwares détectés
- Consulter les forums,(avec un autre PC) des logiciels spécialisés permettent parfois d'éliminer la menace
- Tenter une restauration de l'ordinateur (cours ?)
- Faite appel a un spécialiste pour reformatez le disque dur et réinstaller le système puis utiliser une sauvegarde pour restaurer vos fichiers perdus. Certains malwares vont se loger dans le BIOS, le reformatage du disque dur dans ce cas sera inutile

Actions en cas d'infection

- Ne jamais répondre aux sollicitations
- Faire des copies d'écran (cours?)
- Redémarrer votre PC
- Concernant le navigateur: voir cours ?
  - Purger le cache,
  - Supprimer les cookies,
  - Réinitialiser les paramètres
- Désinstaller les applications suspectes: voir cours?
- Changer les mots de passe : voir cours « mots de passe »
- Si pb avec coordonnées bancaires : faire opposition
- Signaler les faits sur Internet-signalement.gouv.fr

Enlever une barre d'outils parasites de votre navigateur

- Installer « Iobit Uninstaller »
- Pointer sur le menu Bundleware et supprimer les programmes installés sans votre autorisation
- Pointer sur « barres d'outils et modules d'extension » et supprimer les modules suspects
- Réinitialiser votre navigateur:

Chrome/paramètres/paramètres avancés/réinitialiser et nettoyer/nettoyer

puis remettre les paramètres par défaut

La réinitialisation du navigateur, désactive les extensions,

réactivez uniquement celles que vous estimez nécessaires

Supprimer les adwares (pubs intempestives)

- Utiliser les outils adwcleaner et malwarebytes (l'antivirus ne détecte pas les adwares)
- Les adwares peuvent être installés sous forme d'extension sur votre navigateur.
  - Réinitialiser le navigateur (permet de désactiver les extensions)
  - Consulter les extensions
    - Chrome : paramètres/extension : supprimer toutes les extensions inutiles ou inconnues
- Supprimer les programmes inutiles (barres d'outils) par exemple installés sur votre PC (manuellement dans la liste des programmes ou avec adwcleaner)
- Si des anomalies persistent , réinitialiser votre navigateur (paramètres/paramètres avancés/réinitialiser et nettoyer)

Messagerie piratée

- Si vous pouvez accéder à votre compte:
  - Modifier votre mot de passe, (ainsi que sur tous les comptes qui utilisent le même mot de passe)
  - Vérifier si vous avez un report d'adresse mail, le supprimer
  - Vérifier vos contacts et supprimer les contacts inconnus
  - Si la base de vos contacts est vide, aller voir s'ils sont dans la corbeille et restaurer les
- Si vous ne pouvez pas accéder à votre compte, tenter la fonction « mot de passe oublié » si cela ne fonctionne pas, contacter rapidement votre opérateur
- Bloquez les achats pouvant être faits à partir de votre compte
- Prévenez votre banque
- Prévenez vos contacts

Windows 10: comment restaurer une ancienne version

- Dans la barre de recherche windows taper « restauration système »
  - Ouverture d'une fenêtre « propriétés système »
  - Cliquez sur « restauration système »
  - Sélectionner une date

- La restauration système ne fonctionnera que si elle a été activée auparavant (menu configuration)

Obtenez de l'aide avec cybermalveillance.gouv.fr

Les 10 règles de base pour la sécurité numérique

Synthèse : les 10 règles de base

1. **Adopter une politique de mot de passe rigoureuse**
2. **Sauvegarder ses données régulièrement**
3. **Faire ses mises à jour régulièrement**
4. **Se protéger des virus et autres logiciels malveillants**
5. **Évitez les réseaux Wifi publics ou inconnus**
6. **Bien séparer ses usages professionnels et personnels**
7. **Éviter de naviguer sur des sites douteux ou illicites et être vigilant lors du téléchargement d'un fichier**
8. **Contrôler les permissions des comptes utilisateurs**
9. **Être vigilant sur les liens ou les pièces jointes contenus dans des messages électroniques**
10. **Faire attention aux informations personnelles que l'on diffuse sur Internet**