Cybersécurité
cours de base

Cours de base
deuxième partie

- Adwares
- Spywares
- Spams

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 clés USB « commerciales »,
  - Des fausses mises à jour de logiciels (Java, Adobe…)

Mesures préventives contre les adwares

- Voir cours antivirus,
- Utiliser des extensions de navigateur :WOT, Adblock, Ublock origin, Utabs
- Télécharger les logiciels uniquement sur les sites d'origine des fournisseurs,
- Etre vigilant
  - Sur les cases « cochées » lors de l'installation d'un logiciel,
  - Sur les autorisations données aux applications installées sur le téléphone.

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 visitez 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 spywares :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)
  - Bloquer les cookies « tiers »

Comment bloquer les cookies « tiers »

- Ouvrez Chrome et cliquez sur les 3 petits points verticaux en haut à droite
- Paramètres/confidentialité et sécurité/cookies et autres données de site:
  - Cochez » bloquer les cookies tiers »

Un cookie tiers est un logiciel intégré dans votre ordinateur par un site différent du site que vous êtes en train de consulter : il permet d'enregistrer des informations liées à votre navigation sur le site

Comment installer une extension sur Chrome

- Ouvrez Chrome,
- Tapez « chrome web store » dans la barre d'adresse,
- Ouvrez le site chrome.google.com,
- Dans la page qui s'ouvre rechercher l'extension (tapez son nom dans la barre de recherche); télécharger et installer la (ou « ajouter à Chrome »)

Comment contrôler les extensions installées sur Chrome

- Ouvrez Chrome,
- Cliquez sur les 3 petits points en haut à droite,
- Sélectionnez « paramètres »,
- Sélectionnez « extension » dans le menu de gauche,
- La page qui s'ouvre vous présente les extensions installées. Il est possible :
  - D'en connaître les « détails »
  - De les supprimer
  - De les désactiver

Les extensions consomment de la place mémoire en RAM et du temps de calcul
Il ne faut pas en abuser

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)

Comment bloquer un N° de teléphone (avec votre portable Android)

- Ouvrez l'appli « téléphone »
  - Cliquez sur « récent » en bas
  - Cliquez sur le numéro à bloquer
  - Cliquez sur le « i »
  - Cliquez sur « Bloquer » en bas de l'écran
- Autre processus :
  - Appli téléphone/ 3 petits points/paramètres/bloquer des numéros

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 (ex:infosva.org)
- 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,
- Signaler les spams téléphoniques à la plateforme (www.33700.fr), 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

Signaler les Spams (mails) avec Gmail

- La messagerie Gmail possède un filtre antispam chargé de bloquer les messages indésirables
- La fonction s'affine au cours du temps si vous signalez les messages publicitaires passés au travers des mailles du filet
- Dans votre boite de réception, sélectionnez le mail indésirable, et cliquez sur l'icône « signaler comme spam » (point d'exclamation en haut de l'écran)

D'autres messageries comme outlook, orange, permettent aussi de signaler les spams

Les malwares sur Téléphone 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

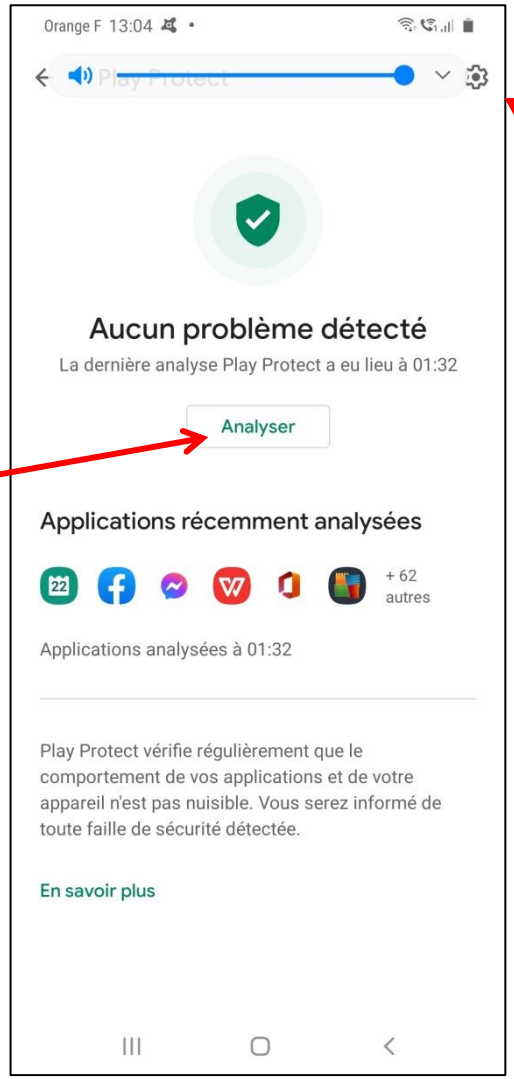
Téléphone: Activer Le Play Protect

- La fonction Google Play Protect contrôle les applications du Play Store avant leur téléchargement,
- Elle détecte les applications potentiellement dangereuses, et supprime les applications nuisibles de l'appareil
- Elle envoie des alertes de confidentialité

Téléphone: Le Play Protect

Play Store/menu/Play protect

Lancer une analyse

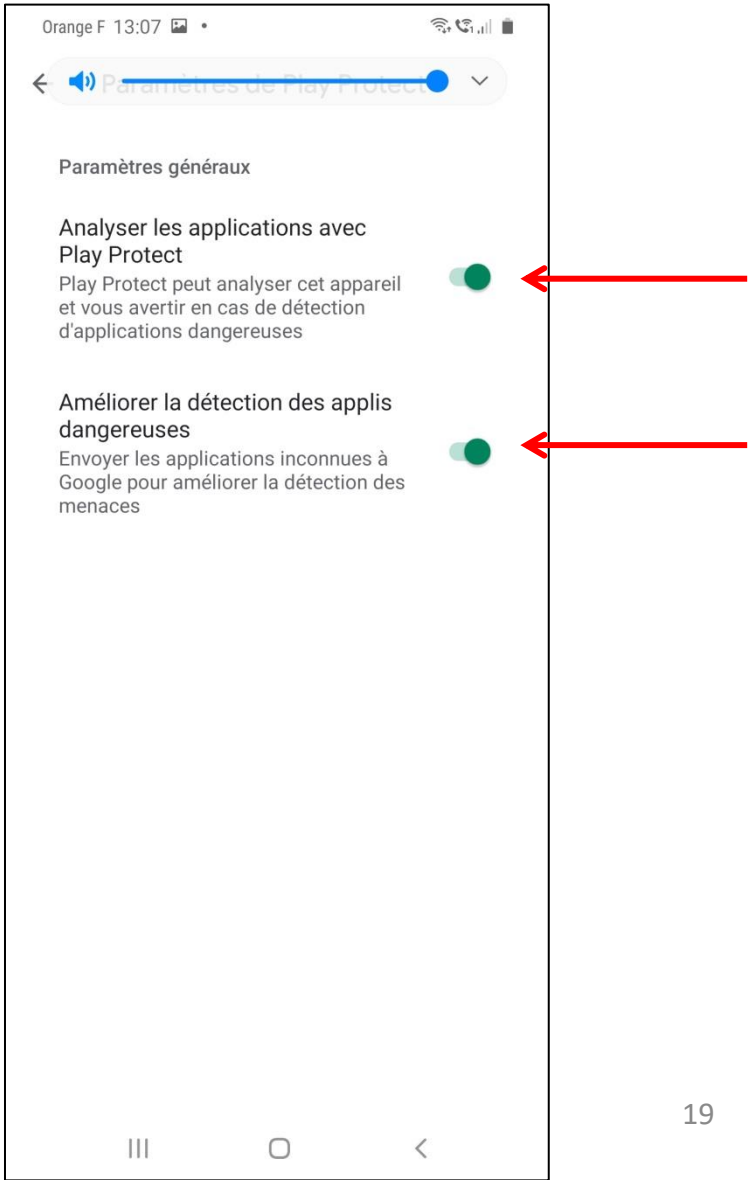


Paramètres
Pour activer ou non le play protect

Téléphone: Le Play Protect

Play Store/menu/Play protect/paramètres

Activation du Play Protect



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 téléchargées,
- 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

- 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)

Fin de la deuxième partie