Cybersécurité
cours de base

Cours de base troisième partie

- La publicité
- Les botnets
- Le chantage à la webcam
- L’hameçonnage
- Ransomwares
- Piratage de messagerie

Comment limiter les publicités

- Principe de fonctionnement des publicités:
  - Les applis sur votre téléphone demandent des autorisations d'accès (contacts, localisation, galerie photos, agenda etc…) lors de leurs installations
  - Certains sites internet installent sur votre PC des cookies d'espionnage (idem applis)

Pendant l'utilisation de vos appareils, des informations sur vos habitudes sont transmises aux organismes de pub (qui achètent ces informations)

Comment limiter les publicités

- Les organismes de pub sont rémunérés pour diffuser de la publicité sur les navigateurs, FB, Youtube etc… (ces sites vendent leurs espaces)
- Les organismes de pub sont rémunérés au »clic» faits sur les pubs affichées, d'où l'intérêt quelles soient ciblées !

Pour limiter les publicités il faut donc agir aux différents niveaux ;

- Limiter les autorisations données aux applications (téléphone),
- Empêcher le chargement de cookies néfastes dans votre navigateur (PC, Téléphone),
- Bien paramétrer les logiciels (facebook par exemple) pour limiter les publicités ciblées
- Supprimer les adwares (outil comme adwcleaner par exemple)
- Tester les appli installées dans le téléphone avec le Play Protect

Comment empêcher les applications d'espionner vos données

- Contrôler les autorisations fournies aux applications, 2 méthodes :
  - Application par application :
    - Paramètres/applications/cliquez sur une application
    - Autorisations (possibilités de modifier)
  - En global :
    - Paramètres/applications/cliquez sur les 3 points/sélectionnez « gestionnaire d'autorisations »
    - Fonction par fonction vous accédez aux applications autorisées (possibilité de modifier)

Comment effacer vos traces numériques

- Lorsque vous utilisez les réseaux sociaux, la navigation sur le web, les recherches, les achats vous laissez des traces; pour les effacer:
  - Nettoyer régulièrement l'historique de navigation,
  - Effacer les cookies
  - Accéder à votre tableau de bord Google et effacer vos traces:
    - Ouvrez Chrome/clic sur votre avatar en haut à droite/gérer votre compte

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 via les paramètres de Windows (gestionnaire de périphériques).

Les botnets

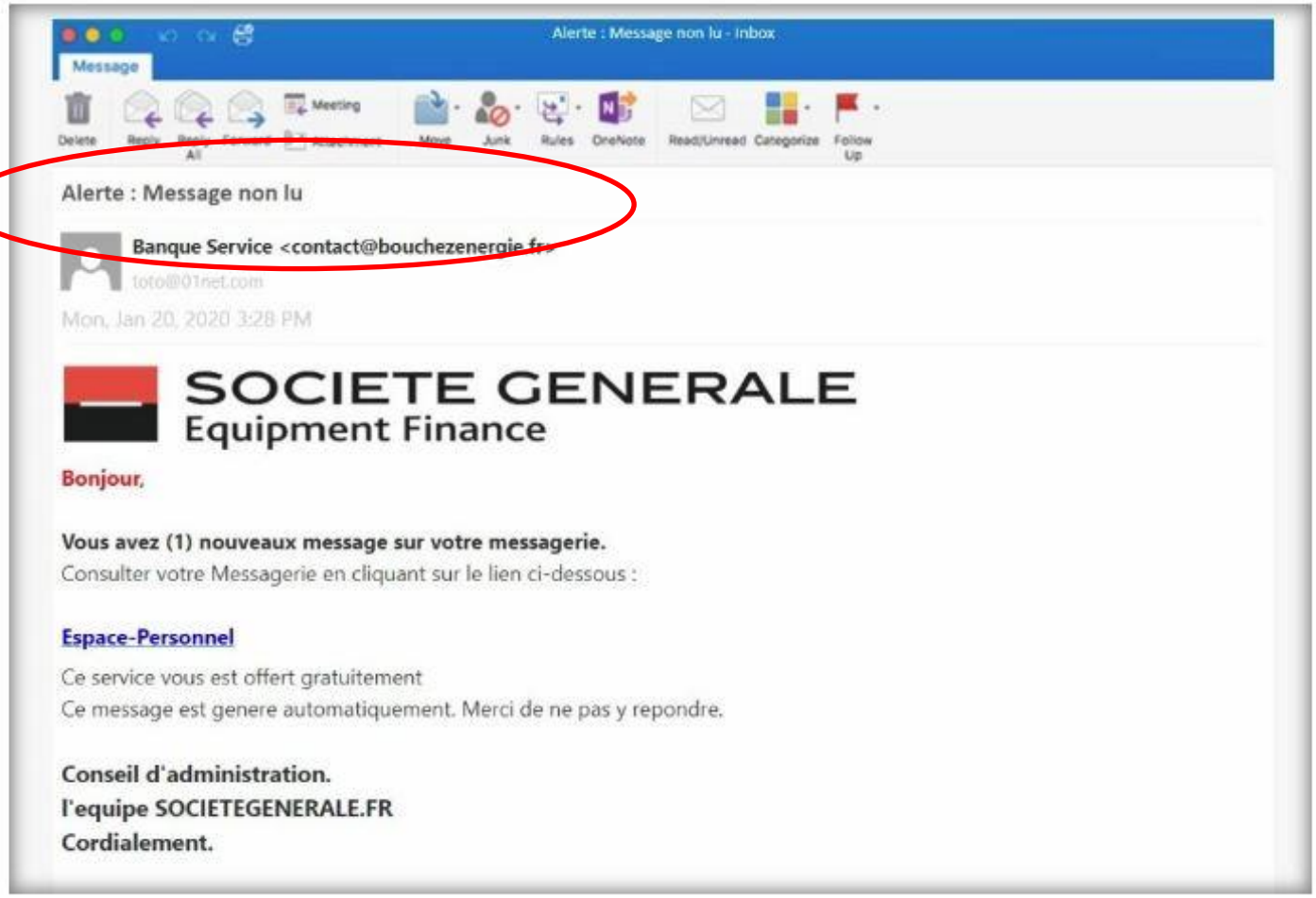
- « robot » et « Network », utilisent une partie de la puissance de l'ordinateur pour participer à des attaques pour rendre indisponible un site web
- Diffusion :mail, téléchargement via un site web infecté
- Principales protections : mettre à jour votre système, vérifier les pièces jointes de mail, 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'énergie, 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

Mesures préventives contre le hameçonnage

- En cas de doute utilisez un service de vérification en ligne comme
- Site d'entraînement à reconnaître le phishing : https://phishingquiz.withgoogle.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

- Rappel du cours messagerie: distinguer « compte » de votre fournisseur d'accès internet (FAI) et vos « comptes de messagerie »
- Voir cours mot de passe et cours messageries
- Appliquer toutes les mesures préventives déjà citées dans ce cours

Se protéger des piratages 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

Règles de base pour protéger vos informations personnelles (synthèse)

- Choisissez un mot de passe sûr en alternant les majuscules et minuscules, les chiffres etc.
- N'utilisez pas un mot de passe unique sur tous vos comptes, alternez en fonction des sites
- Ne partagez pas vos mots de passe et prenez vos précautions lors de leur utilisation sur d'autres ordinateurs que le vôtre
- Vérifiez l'authenticité d'un expéditeur avant d'envoyer des informations personnelles ou sensibles par mail
- Evitez d'inscrire votre adresse mail principale sur des sites dont vous n'êtes pas sûr
- Soyez attentif à vos relevés de compte bancaire

Fin de la troisième partie