Activité Sécurité de navigation_éléments de correction.

Mise en situation

***Q.1 et Q.2** : toute réponse pertinente est acceptée ici (utilisation de l'historique de navigation, stockage de donnés non voulues sur l'ordinateur ET des serveurs extérieurs etc.)*

Historique de navigation

***Q.1** : il faut l'effacer assez régulièrement (avec toutes les options) car des robots peuvent s'en servir et proposer des publicités non voulues voire envoyer des emails. C'est aussi une sécurité car cette action supprime les pseudos / mots de passe voire numéros de cartes bleues enregistrés.*

***Q.2** : ni l'un, ni l'autre. Effacer l'historique et supprimer un fichier installé sont deux opérations différentes. D'ailleurs, certains logiciels désinstallés (la plupart du temps non voulus) peuvent même se réinstaller tout seul une fois supprimés !*

Qu'est-ce qu'un cookie ?

***Q.1** : un cookie est un petit fichier stockant des données relatives aux pages visitées d'un site mais aussi des données personnelles comme des mots de passes ou pire des numéros de cartes bleues. Le cookie peut aussi parcourir l'historique de navigation et ... envoyer faire envoyer des publicités etc. Certains sites obligent l'utilisateur à avoir des cookies sans demander l'autorisation (alors que c'est obligatoire).*

L'intérêt d'un cookie est d'accéder à ses sites préférés plus rapidement (par exemple, on peut retrouver sa page Facebook sans rentrer à chaque fois son mot de passe). Il faut donc les effacer régulièrement mais ne pas refuser ceux qui sont liés aux sites préférés sinon, il se peut qu'on l'on ne puisse pas y accéder complètement.

***Q.2** : effacer les cookies (en général, c'est l'option par défaut lorsque l'on supprime l'historique de navigation) a deux conséquences : un accès plus lent aux sites et la disparition de certaines publicités.*

Malheureusement, certains sites stockent sur leurs serveurs -et à notre insu- notre adresse IP, nos adresses mails, nos favoris notamment, ce qui ne supprime pas tout passage sur le Web. Pour cela, il faut opter pour une navigation privée (offerte par certains navigateurs comme Opéra) ou mieux un VPN qui permet d'attribuer une adresse IP fictive et donc ne pas être suivi facilement. Aucune protection n'est fiable à 100%.

Des vigilances pour éviter la capture de données

***Q.1** : une adresse URL indique le protocole utilisé, le serveur, le dossier et la page visitée (voir cours).*

***Q.2** : des logiciels non demandés sont proposés en téléchargement, certains produits s'avèrent payants au bout d'une période d'essai, de publicités (sponsors) apparaissent, des logiciels espions (spyware) peuvent aussi être téléchargés à l'insu de l'utilisateur et envoyer des données à des sites. Le site propose aussi d'autres logiciels à installer en plus de celui télécharger, il faut donc être vigilant.*

<u>Q.3</u> : pas de cases à décocher dans cette nouvelle version attention à ne télécharger que le logiciel souhaité.

Il ne faut surtout pas cliquer sur le lien d'un mail douteux (risque important de malware, trojans etc.) et s'il s'agit d'un phishing (mail ressemblant à celui de sa banque par exemple) avertir l'organisme en question et l'effacer. Il existe également de sites gouvernementaux permettant d'indiquer les spams et mails douteux.

Penser également à utiliser un antivirus + antimalware de temps en temps sur l'ordinateur pour supprimer certains fichiers douteux qui pourraient mettre en cause son intégrité et le rendre plus fragile face à des pirates.

L'utilisation d'un pare-feu est vivement recommandée car il permet d'éviter que de tierces personnes écoutent certaines communications sensibles en bloquant l'ouverture de ports non désirés.

Enfin, la navigation privée (proposée gratuitement par certains navigateurs comme Opéra) limite également les risques de piratage sur Internet.