Livret de synthèse élève

Définitions :

Phishing : pratique malveillante visant à récupérer des informations personnelles sur une cible (ex : envoie d’un mail malveillant à un grand nombre de personnes). Le spear phishing personnalise le support d’attaque en fonction de la cible (ex : nom de la cible présent dans le mail malveillant)

Ransomware : programme malveillant dont la fonction est de chiffrer les données du support attaqué (rendant les données illisibles). La clefs de déchiffrement est proposée en échange d’une rançon. Il ne faut en aucun cas payer cette rançon !!

Virus : programme malveillant ayant la propriété de s’auto-répliquer se propageant ainsi dans le système informatique.

Authentification : procédé permettant de s’assurer de l’identité de la personne qui cherche à utiliser un système. Attention : un identifiant n’est pas un authentifiant, n’importe qui peut connaître un identifiant, c’est le mot de passe (par exemple) qui permet d’authentifier.

Hashage : application d’une fonction mathématique (fonction de hash) à une suite de mots ou de lettres. Le résultat de cette fonction, le hash, est une autre suite de caractères n’ayant rien à voir avec la première. La fonction de hash utilisée a deux propriétés importantes : un petit changement dans la suite de caractère entrée entraîne de gros changements dans le résultat, et il est impossible de déduire la suite de caractère entrée à partir du hash. Cette technique est beaucoup utilisée par exemple pour le stockage des mots de passe : lors de la création du compte, le hash du mot de passe est calculé et stocké, puis à chaque connexion le hash du mot de passe entré est calculé et comparé avec celui stocké, si les hash correspondent alors le mot de passe est le bon.

Chiffrement : transformation des données à travers une fonction mathématique. Cette transformation est réversible en utilisant la clef de déchiffrement qui correspond.

Cookies :  Un **cookie** est un petit fichier très **simple**, en fait un texte, enregistré sur le disque dur de l'ordinateur d'un internaute à la demande du serveur gérant le site Web visité. Il contient des informations sur la navigation effectuée sur les pages de ce site.

Données personnelles : ensemble des informations permettant d’identifier quelqu’un de manière directe ou indirecte.

Cloud : stockage de documents sur des serveurs permettant l’accès à ces documents à distance et sur différents supports.

Neutralité du net : grand principe définissant l’égalité et l’équité sur internet. Par exemple un site internet ne peut pas être avantagé ou désavantagé par rapport à un autre. On ne considère cette question qu’au niveau des structure de l’Internet globale, car par exemple lors d’une recherche certains sites seront plus facilement trouvés que d’autres (on dit qu’ils sont mieux indexés), cependant cela ne relève pas de la neutralité du net.

Usurpation d’identité : récolte de données personnelles et utilisation de celles-ci dans le but de se faire passer pour le propriétaire de ces données. L’usurpation d’identité est punie d’un an de prison et de 15 000 € d’amende.

Data Center : bâtiment abritant des « fermes de serveurs », ils servent de relais ou de sources d’informations. Par exemple une grande entreprise (Amazon par exemple) dispose de plusieurs data center stockant toutes ces données et permettant entre autres l’accessibilité de ces données via internet.

Lumière bleue : type de lumière émise en grande quantité par le soleil mais également par les écrans LED et LCD. Ces lumières peuvent perturber le cycle de sommeil si elles sont reçues peu de temps avant de se coucher (notre cerveau pense qu’il fait encore jour). Elles sont également source de fatigue pour les yeux. Il est recommandé d’éteindre les écrans au minimum 30 minutes avant de se coucher. Il est également conseillé d’activer les filtres à lumière bleus sur les appareils proposant cette fonctionnalité ou de porter des lunettes portant ce filtre (lunettes spécifiques ou filtre intégré sur les lunettes de vues).