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).

# Quels sont les bons comportements à adopter ?

* **En cas de doute sur les intentions d’un message reçu, le plus simple est de ne pas donner suite**. Si ce doute arrive dans un second temps, **il n’est jamais trop tard : parlez-en autour de vous** à des personnes de confiance. Selon les cas, un signalement sur le site [www.internet-signalement.gouv.fr](http://www.internet-signalement.gouv.fr/) peut être fait et de l'aide peut être apportée via le site [www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr/).
* De manière plus générale : **vous n’êtes pas seuls !** Victime ou témoin de comportements anormaux, il est nécessaire et important d’en parler pour trouver des solutions : vos parents, le signalement, les cellules d’écoute
* **Restreindre aux seules personnes de confiance les informations personnelles ou sensibles que vous ne voudriez pas voir diffusées sur Internet** : ne pas communiquer ces informations à des inconnus, configurer ses paramètres de sécurité et confidentialité sur les réseaux sociaux, désactiver la géolocalisation des photos partagées publiquement, etc.
* **Protéger l’accès à vos comptes** : vos **mots de passe** doivent rester secrets en toute circonstance, **compliqués à deviner pour les autres et faciles à retenir par vous**. Ils ne doivent pas être partagés et doivent régulièrement être changés, par précaution. Pour qu’ils soient plus sécurisés, préférez les mots de passe longs aux courts et faîtes une combinaison de lettres minuscules, majuscules, chiffres et caractères spéciaux.

## Amis virtuels :

* Sur Internet, il est difficile de concrètement savoir qui se cache derrière vos amis virtuels (derrière des pseudonymes, des avatars, etc.).
* **Ne partagez aucune donnée privée sur vous ou sur votre famille avec un inconnu. N’acceptez pas de rendez-vous dans la vraie vie d’inconnus rencontrés sur Internet.**
* En cas de doute sur l’identité de vos amis virtuels et/ou sur le type de discussion(s) que vous entretenez, n’hésitez pas à **en discuter avec vos parents ou un tiers de confiance** (professeurs, CPE, oncles et tantes, grands-parents, fratrie, etc.).

## Cyberharcèlement :

* Le cyberharcèlement est un effet de groupe visant à nuire (insultes, moqueries, agression, etc.), et ce à l'encontre d'une personne souvent isolée, via les canaux numériques et dans la durée.
* **Ne participez en aucun cas au mouvement de cyberharcèlement** car cela peut s’avérer très dangereux ! Il peut provoquer suicide, anxiété, déscolarisation, replis sur soi, exclusion, dépression, etc.
* Aussi, si vous êtes victime, ou témoin d’une situation de cyberharcèlement, **n’hésitez pas à le signaler, et/ou à en discuter avec quelqu’un de confiance** (parents, professeurs, CPE, oncles et tantes, grands-parents, fratrie, etc.). La plateforme NetEcoute permet aussi de se confier et de signaler ses problèmes

## Phishing :

* Des attaquants peuvent utiliser la toile afin de vous tendre des pièges . Que ce soit par mail, SMS ou tchat, il faut rester vigilant lorsque l’on reçoit un message invitant à cliquer sur un lien ou un document. Celui-ci peut être piégé !
* Pour déceler les pièges, prêtez attention entre autres aux points suivants : l’adresse de l’émetteur, le contenu, la structure du lien si lieu est (en cas de doute, cherchez l’organisme sur un moteur de recherche, utilisez l’adresse obtenue et vérifiez si sa structure correspond à celle reçue).
* Quoi qu’il en soit, **n’ouvrez pas de pièces jointes et ne cliquez pas sur des liens contenus dans des mails provenant d’un inconnu et/ou qui vous paraissent douteux** (fautes d’orthographe, cadeaux exceptionnels, etc.). Cela peut mener à des arnaques, à des fraudes et à des virus qui viendront bloquer votre appareil électronique.
* **Si vous vous êtes fait piéger, ne cherchez pas à le cacher**: parlez-en avec vos parents ou un tiers de confiance (professeurs, CPE, oncles et tantes, grands-parents, fratrie, etc).

## Challenges :

* Les challenges, ou défis en ligne, sont une pratique très répandue. Récemment deux cas concrets de challenge sévissent en ligne (cf. encadré).
* Si jamais un inconnu vous aborde en ligne, ou même une connaissance voire un ami et vous demande de relever des défis de ce type, **le premier réflexe à avoir est d’en discuter avec quelqu’un de confiance** (parents, professeurs, CPE, oncles et tantes, grands-parents, fratrie, etc).

## Chantage :

* Un internaute malintentionné, peut rentrer en contact avec vous et vous demander certaines données (type données bancaires pour faire des achats), voire vous demander de relever des défis (du plus simple au plus tordu). Si vous ne répondez pas positivement à ses demandes, celui-ci vous menace de dévoiler des informations privées à votre propos, vos secrets par exemple (les communiquer à vos contacts Instagram, par mail ou à vos parents).
* Si **jamais vous êtes victime de ce genre de pratiques, ne répondez pas, ne payez rien, conservez les preuves** (captures d’écran, mails, etc.), **et trouvez de l'assistance sur le site** [**www.cybermalveillance.gouv.fr**](http://www.cybermalveillance.gouv.fr/).
* Surtout, parlez-en avec vos parents ou un tiers de confiance (professeurs, CPE, oncles et tantes, grands-parents, fratrie, etc.

## Vie privée :

* Afin de conserver votre vie privée sur Internet, quelques bonnes pratiques à adopter :
* Par défaut, ce que vous publiez sur les réseaux sociaux est accessible à tout le monde : vérifiez bien les paramètres de « confidentialité » ou « sécurité » et réglez-les pour être sûr que seuls vos amis ont accès à vos données.
* **Réfléchissez méticuleusement aux données que vous partagez sur Internet** : âge, données bancaires (les vôtre ou celles de vos parents), adresse postale, opinions politiques, religieuses, etc.
* **Désactivez la géolocalisation lorsque vous prenez des photos**. Lorsque vous postez une photo en ligne, celle-ci comporte ce que nous appelons des « métadonnées » dont votre géolocalisation ! Cela signifie que toute personne ayant accès aux photos publiées peut savoir où la photo a été prise et donc où vous vous trouvez à un instant T. Très pratique pour un cambrioleur qui veut savoir si vous êtes chez vous par exemple.
* Aussi, il est important de **garder en tête qu’Internet a la mémoire longue !** Tout ce que vous postez aujourd’hui alimente ce que l’on appelle votre e-réputation et pourra impacter votre futur. Ainsi, réfléchissez bien à deux fois avant de publier du contenu.

## Fake news :

* De fausses informations circulent sur Internet… Bien sûr puisque n’importe qui peut y poster ce qu’il souhaite !
* Ainsi, avant de relayer des informations, ou avant d’utiliser du contenu (pour des exposés par exemple), **il est important de vérifier et croiser les informations que vous trouvez sur Internet**. En cas de doute, n’hésitez pas à en parler avec vos parents ou un tiers de confiance (professeurs, CPE, oncles et tantes, grands-parents, fratrie, etc.).

## Mot de passe :

* Les mots de passe protègent l’accès à vos comptes et donc à vos données : ils doivent rester secrets si vous ne souhaitez pas que des personnes mal intentionnées usurpent votre identité ou volent vos informations.
* Il faut choisir des mots de passe à la fois compliqués à deviner pour les autres et faciles à retenir pour vous.
* **Avoir un mot de passe différent par site ou application réduit aussi les risques de se faire voler ses mots de passe.**
* Ne les partagez pas et ne les écrivez pas sur un papier. Enfin, changez de mot de passe régulièrement, par précaution.
* Restez particulièrement vigilant pour le mot de passe de votre adresse mail. Si celui-ci est compromis, cela permettrait aux hackers de réinitialiser vos mots de passe sur vos différents comptes et d’accéder aux sites sur lesquels vous êtes inscrits

## Signalement :

* Sur Internet, vous pouvez être confronté(e), sans le vouloir, à du contenu choquant. Si cela vous arrive, vous pouvez signaler le contenu : directement sur le site si possible (Facebook, Instagram, etc.) ou via la plateforme de signalement PHAROS ([www.internet-signalement.gouv.fr](http://www.internet-signalement.gouv.fr/)).
* **Si un contenu vous a choqué, il est important de ne pas se sentir gêné d’en discuter avec un tiers de confiance** (professeurs, CPE, oncles et tantes, parents, grands-parents, fratrie, etc).
* De même, sur Internet, vous disposez d’un droit sur les photos où vous êtes identifiable ! Ainsi, si **une photo de vous circule et vous dérange, n’hésitez pas à signaler le contenu** et / ou à en discuter avec vos parents ou tout autre personne de confiance.

## Cellule d’écoute :

* Il est important d’échanger sur nos expériences d’Internet !
* **Si** **jamais vous êtes victime, témoin ou acteur de l’une des situations précédemment évoquées, il faut en discuter !**
* Si vous ne souhaitez pas en discuter avec vos proches, il est possible d’appeler le numéro qui est inscrit sur votre livret. Vous pourrez en parler en tout anonymat et recevoir des conseils.

# Ressources à disposition :

**Net Ecoute :**

Site de sensibilisation aux dangers du net : <https://www.netecoute.fr/> (possibilité de discuter via un chatbot)

Numéro de téléphone : 0800 200 000

**PHAROS (plateforme de signalement de contenu) :**

<https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action>

**Plateforme de sensibilisation et d’aide aux victimes (cybermalveillance) :**

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

La plateforme en ligne Cybermalveillance.gouv.fr assure un accompagnement à deux niveaux :

* **Vous êtes victimes d'actes de cybermalveillance (escroqueries, piratage de comptes...) ?** Cybermalveillance.gouv.fr fait un **diagnostic précis de votre situation et vous met en relation**, le cas échéant, avec les spécialistes et organismes compétents proches de chez vous
* **Vous souhaitez comprendre les risques numériques et savoir comment réagir ou adopter les bonnes pratiques ?** Cybermalveillance.gouv.fr met à disposition **des outils de sensibilisation et de nombreux conseils** sur des thématiques du quotidien, et sous différents formats (vidéos, fiches réflexes, mémos, bandes-dessinées...).

