LIVRET EXPLICATIF ET D'ACCOMPAGNEMENT

ACCOMPAGNEMENT À L'ESCAPE GAME

EXPLICATION DES NOTIONS

UNIVERSITÉ DE NAMUR

Par groupe de 3

50 minutes maximum

Elèves du premier degré du secondaire

Ce livret explicatif a pour but d'accompagner la mise en place d'un escape game numérique à destination des élèves du premier degré du secondaire. Il contient toutes les informations nécessaires à sa mise en place, à sa supervision, et à son suivi.

ATTENTION

Cet outil visant la sensibilisation à la cybersécurité est en cours d'expérimentation dans le cadre de la réalisation d'un mémoire. Il a déjà été testé, mais jamais en environnement scolaire. Veuillez nous excuser pour tout dysfonctionnement ou manquement dans la documentation qui va suivre.

printemps des sciences 21

UNIVERSITÉ DE NAMUR

Présentation

L'escape game se présente sous la forme d'un programme à exécuter sur un ordinateur. Il propose aux élèves d'incarner des experts de la cybersécurité, enquêtant sur la disparition des bulletins. A travers un voyage 'simulé' dans l'ordinateur du directeur de l'établissement dont les bulletins ont disparu, les élèves, par groupe, seront amenés à questionner certaines mauvaises pratiques, comprendre de nouveaux concepts, ou encore prendre conscience de leur empreinte numérique.

Toute l'enquête est rythmée par un assistant personnel présent en bas de l'écran, donnant des conseils ou aidant à la résolution d'énigmes.

Mise en place

L'activité est proposée pour des groupes de deux ou trois élèves qui prendront place devant un ordinateur.

Afin de préparer l'activité, il faut, pour chaque poste :

- Exécuter le programme de l'escape game
- Placer un post-it sur lequel vous aurez écrit « 4862 ».

Pour exécuter le programme, il faut d'abord copier le fichier présent sur la clé usb appelé « os.exe » et le coller sur chaque ordinateur, peu importe l'endroit.

Ensuite, il suffit de cliquer dessus pour qu'il charge. Une petite animation peut rester plusieurs secondes avant de disparaître et laisser place au jeu en tant que tel.

L'utilité du post-it sera expliquée dans le scénario.

Il est important de tester l'exécution avant de commencer l'activité.

Difficulté potentielle :

Il est possible qu'un antivirus scanne le fichier avant de permettre son exécution sur l'ordinateur, même si celui-ci ne nécessite pas d'installation.
Jusqu'ici, toute exécution a pu être menée à bien, mais en cas de problème, vous pouvez être amené à demander de l'aide à un responsable de votre cyber-classe.

En résumé, la mise en place requiert deux préparations :

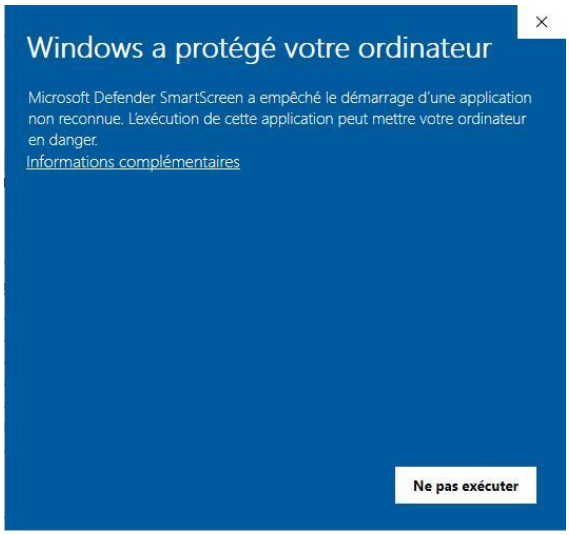
- ✓ Mise en place du fichier à exécuter et exécution de celui-ci sur chaque ordinateur
- ✓ Dépôt d'un post-it sur lequel « 4862 » est écrit à côté de chaque ordinateur

! Un essai de l'exécution est conseillé avant l'activité.

Problèmes possibles

Il est possible que votre antivirus, ou une protection de windows, appelée *windows defender*, veuille empêcher l'exécution du programme. Etant sans danger, la plupart des antivirus et autres protections l'analyseront avant de le laisser s'exécuter. En revanche, une petite manipulation est peut-être nécessaire.

Windows defender



Si vous obtenez cette erreur, il vous faut cliquer sur « informations complémentaires » situé à la fin du paragraphe. Vous obtiendrez alors la seconde image, vous permettant de cliquer sur « exécuter quand même ».

Première étape

Durant la première étape, un problème a été rencontré au moment de cliquer sur les trois éléments étranges du mail.

Il s'agit d'un problème d'affichage rendant le bouton servant à passer à la suite invisible. Il semblerait qu'en cliquant sur différentes parties du mail, le bouton fini par être actionné.

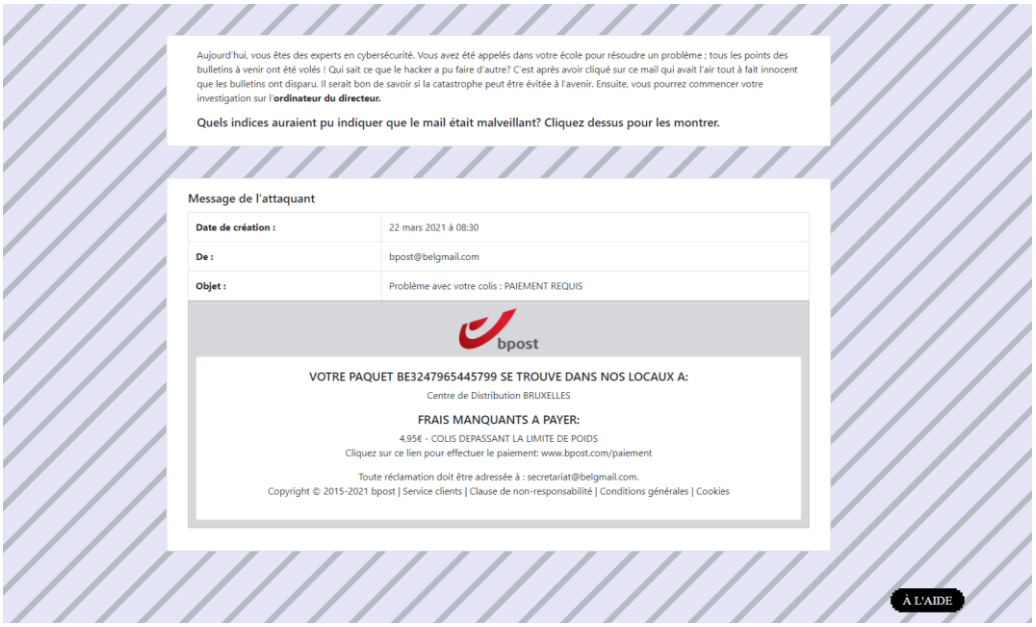
Ce problème n'ayant eu lieu qu'une seule fois, il a été difficile de le régler, et bien que des changements aient eu lieu, il est toujours possible de le voir réapparaître.

Scénario et déroulement

Cette section a pour but de décrire le scénario ; toute notions complexe sera expliqué ensuite dans la section « Objectifs d'apprentissage et notions abordées ».

Pour garder le secret, vous pouvez essayer le jeu par vous-même d'abord.

1ère étape :



Objectif

Prendre conscience du danger que peut représenter un mail

Trouver les éléments distinctifs du phishing

Les enquêteurs se trouvent face à un exercice préliminaire.

Il faut cliquer sur les éléments du mail qui leur paraissent suspects jusqu'à trouver les trois réponses. Une aide est disponible en bas de l'écran.

Celles-ci sont :

- ✓ L'adresse mail bpost@belgmail.com
- ✓ L'objet Problème avec votre colis : PAIEMENT REQUIS
- ✓ Le message 4,95€ - colis dépassant la limite de poids

Les réponses trouvées, l'enquête commence.

2ème étape

Objectif

Découvrir une mauvaise pratique liée à la gestion des mots de passe

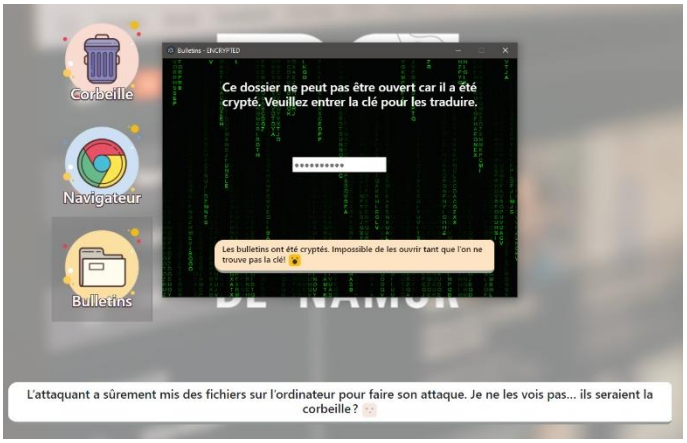
Se sensibiliser aux risques de la fuite de mot de passe

Les enquêteurs se retrouvent face à l'interface représentant l'écran de verrouillage de l'ordinateur qui a été infecté, c'est-à-dire celui du directeur.

Une aide est disponible en bas de la page au besoin.

Pour résoudre cette énigme, il faut trouver le **post-it** présent sur la table et introduire le code, qui se trouve être « 4862 ». La session du directeur s'ouvre et les enquêteurs arrivent sur le bureau de son ordinateur.

3ème étape



Objectif

Apprendre la notion de cryptographie

En cliquant sur le dossier devant contenir les bulletins, les enquêteurs apprennent que ceux-ci ont en fait été chiffrés, c'est-à-dire qu'ils ne sont plus lisibles par l'ordinateur, et donc, par l'utilisateur. Ceci constitue l'énigme principale. L'objectif est alors de trouver le code permettant de les déchiffrer.

Pour ce faire, l'assistant personnel au bas de l'écran suggère d'aller voir dans la corbeille.

4ème étape

Objectif

Apprendre l'existence de la récupération de données et de la persistance des données

Après avoir ouvert la corbeille, l'assistant suggère la récupération de données. En cliquant sur le bouton dédié à cela, un message apparaît effectivement dans la corbeille.

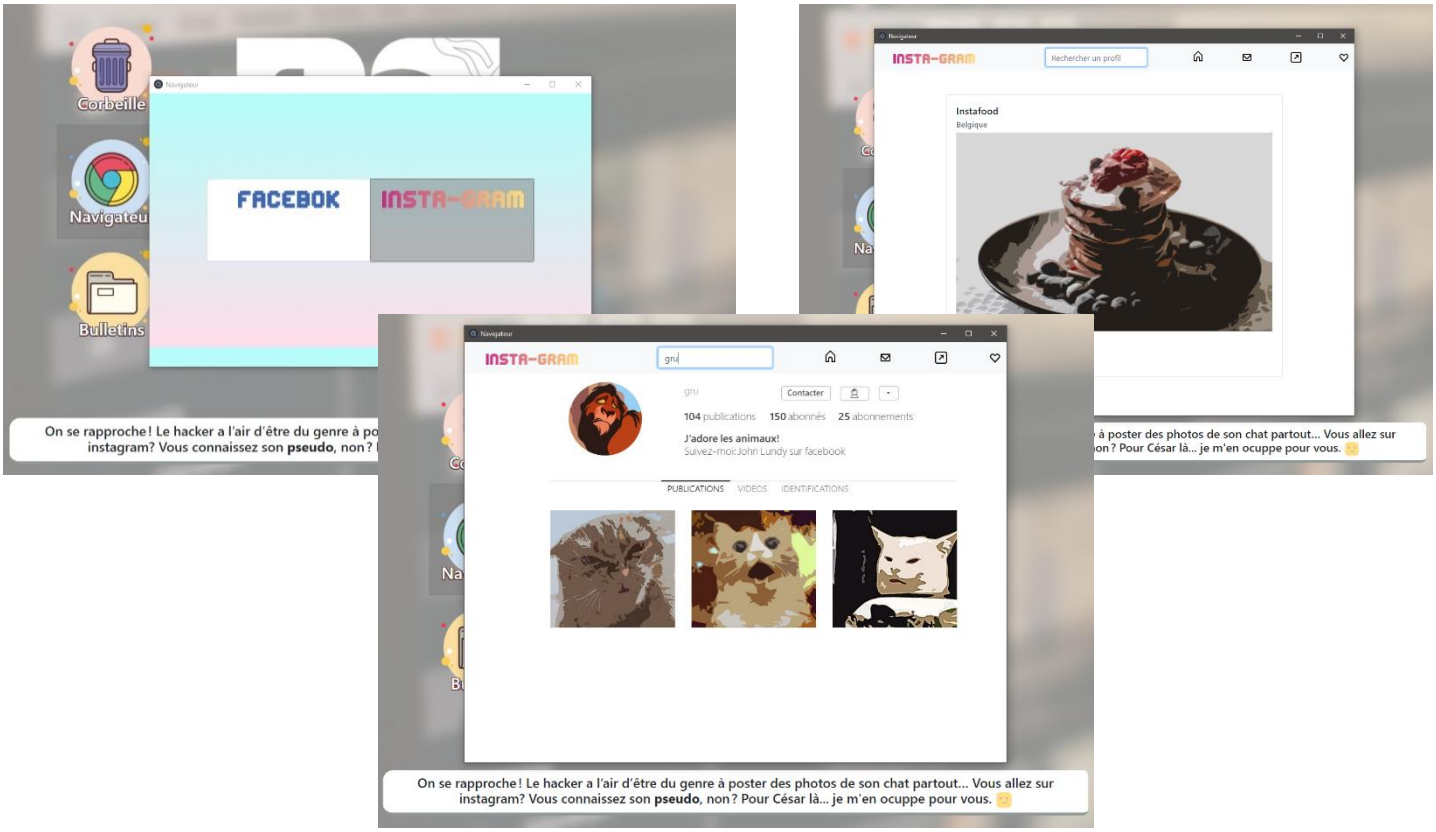
5ème étape

En cliquant sur la note, les enquêteurs apprennent qu'il s'agit d'une note laissée par le hacker sur l'ordinateur. Il permet de connaître les deux composants du code :

- ✓ Le nom du chat du hacker
- ✓ Un mot de passe facile à 5 chiffres

Le tout est chiffré grâce à un chiffrement de César. L'assistant propose d'utiliser le pseudo du fond de la note sur insta-gram, et cherche une explication pour le chiffrement de César lui-même.

6ème étape



Objectif

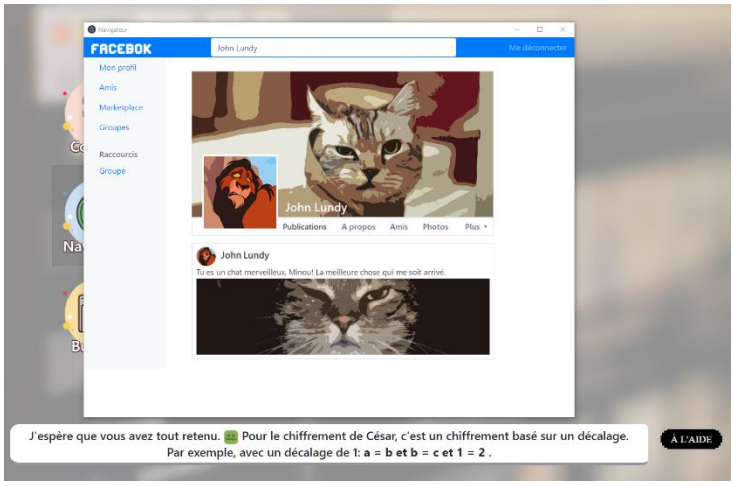
Découvrir un aperçu de l'empreinte numérique

Observer la notion d'anonymat sur internet

Comme l'assistant l'a proposé, les enquêteurs cherchent le pseudo de Gru dans insta-gram.

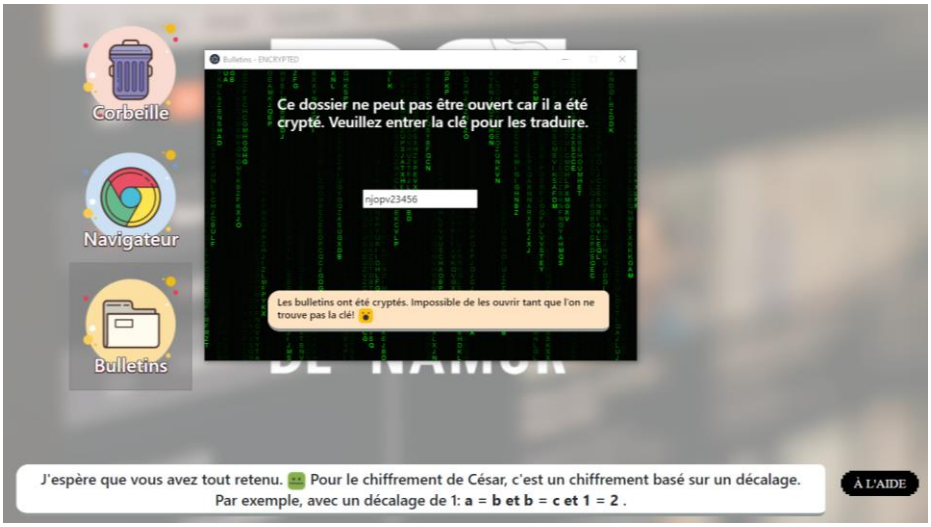
L'étape suivante peut être difficile car l'assistant ne la cite pas tout de suite. Les enquêteurs doivent déduire par eux-mêmes l'intérêt d'avoir trouvé le vrai nom du hacker. Une aide de votre part peut être requise.

7ème étape



Cette étape permet d'obtenir le nom du chat du hacker, c'est-à-dire minou, en recherchant le vrai nom du hacker sur Facebok.

8ème étape



Objectif

Comprendre l'intérêt d'un mot de passe complexe

Apprendre le fonctionnement du chiffrement de César

Il s'agit de l'énigme la plus difficile de l'enquête. En effet, il faut d'abord appliquer le décalage au mot « minou ». Il faut ensuite ajouter au résultat un mot de passe facile à 5 chiffres, c'est-à-dire « 12345 » ayant aussi subi un décalage, c'est-à-dire « 23456 ».

✓ Le mot de passe est donc « **njopv23456** »

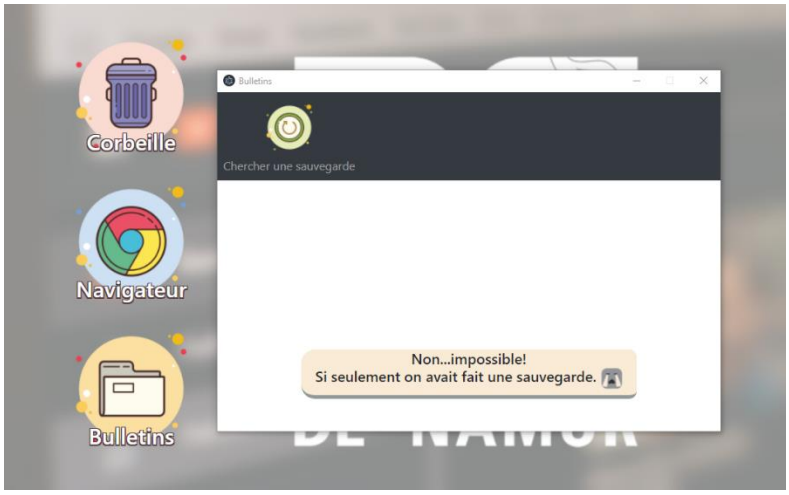
Cette étape est effectivement complexe, mais la complexité est volontaire dans le sens où elle permet d'observer l'intérêt d'un mot de passe compliqué.

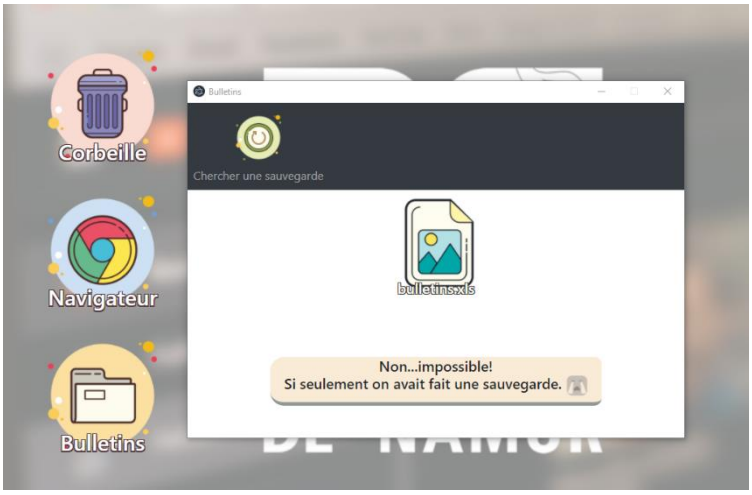
Cette étape étant difficile, une mesure du nombre de lettres correctes a été ajouté. Cependant, l'objectif n'est pas de trouver la réponse par essai-erreur. Cette fonctionnalité ne le permet pas.

Les erreurs sont souvent celles-ci ;

- Ne pas crypter la moitié du mot de passe : minou23456 ou njopv12345
- Oublier la moitié du mot de passe : minou, 12345, njopv ou 23456

9ème étape





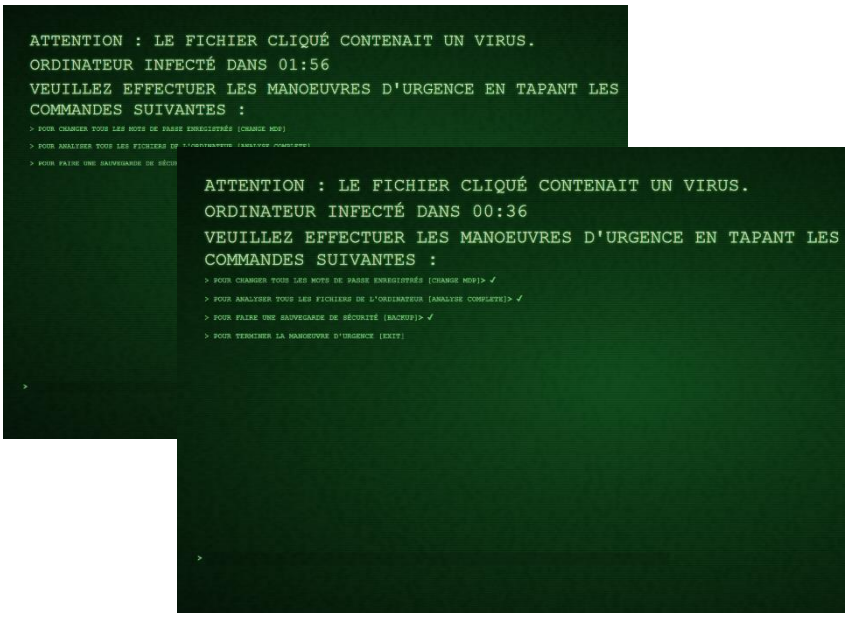
Objectif

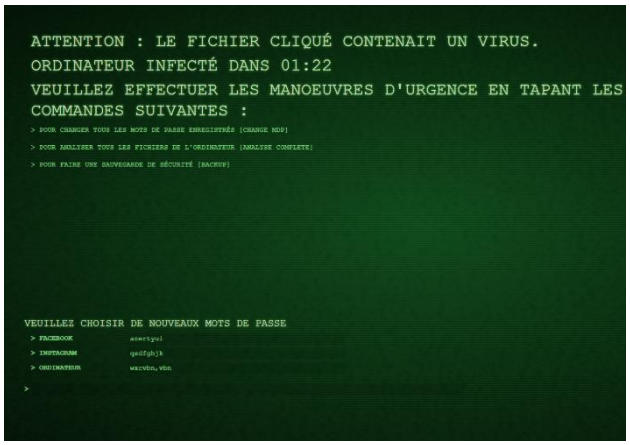
Apprendre l'importance de faire des sauvegardes de sécurité

Les enquêteurs doivent appuyer sur « chercher une sauvegarde » afin de faire apparaître un fichier dans le dossier dans lequel les bulletins devaient se trouver.

Ensuite, il suffit de cliquer sur le fichier.

10ème étape





Objectif

Se familiariser avec les bonnes pratiques de mot de passe, d'analyse de virus et de sauvegarde de sécurité

Les enquêteurs se trouvent devant un terminal parce que le fichier cliqué était infecté. Il faut, pour réussir et terminer l'escape game, réaliser des actions qui sont de bonnes pratiques sur l'ordinateur. Pour ce faire, 3 commandes doivent être tapées dans l'espace en bas :

- ✓ Change mdp
- ✓ Analyse complete
- ✓ Backup

Change mdp donnera lieu à un changement de mots de passe ; des mots de passe différents et suffisamment longs devront être entrés.

Les autres donneront lieu, respectivement, à un temps d'attente pour analyse, et à l'autre, à un temps d'attente pour réaliser la sauvegarde des fichiers de l'ordinateur.

Objectifs d'apprentissage et notions abordées

Bonnes pratiques

Les bonnes pratiques à adopter en ligne et, de manière plus générale, sur l'ordinateur ou tout appareil permettent d'éviter bien des désagréments. Ceux-ci peuvent varier de la perte de données à leur divulgation en passant tout simplement par l'impossibilité d'utiliser un service ou un appareil.

Les grandes entreprises ne sont pas les seules à devoir se protéger ; les conséquences financières de certaines attaques sont impressionnantes, mais tout à chacun doit également savoir se protéger, ne serait-ce que pour éviter de voir son compte cracké ou pour éviter le désagrément de perdre ses dossiers après avoir mis un ordinateur hors d'usage.

Dans cet escape game, seules quelques bonnes pratiques sont citées, mais pour plus d'informations, il existe beaucoup de documentation en ligne telle que celle-ci :

https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf

Chiffrement de césar

Pour commencer, le chiffrement est un procédé qui repose sur un algorithme, c'est-à-dire des étapes à suivre, qui permettent d'éviter que le document puisse être lu par des entités qui n'ont pas la clé permettant de le lire.

En d'autres termes, chiffrer signifie modifier le fichier pour le rendre illisible, et la seule manière de le lire est d'avoir un élément, appelé une clé, qui permet de traduire le document pour lui rendre son apparence initiale.

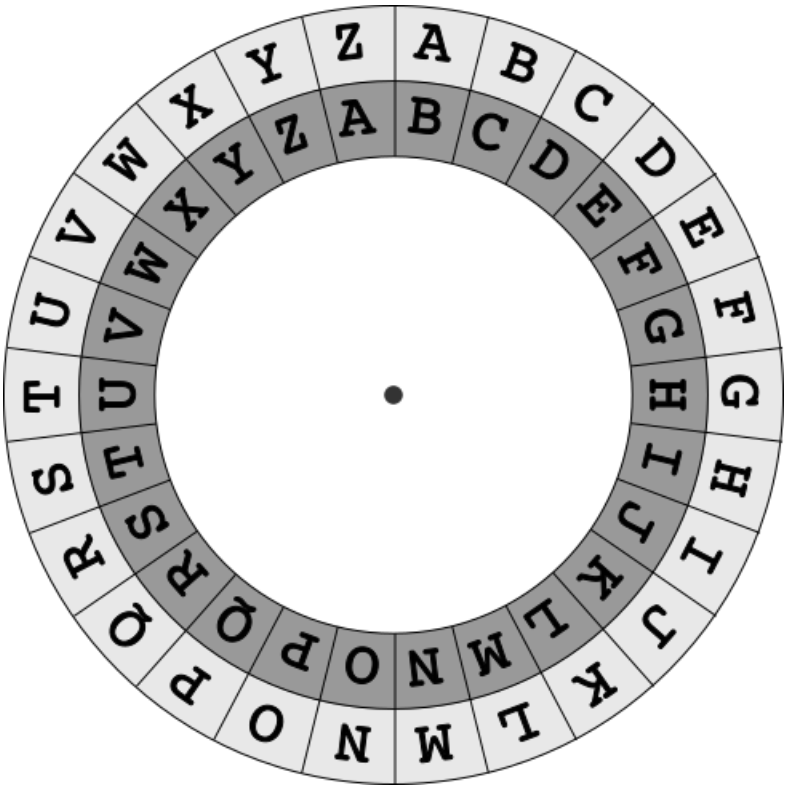
Cela est utilisé, par exemple, par les systèmes qui envoient des messages sur internet ; si une personne malveillante parvient à capter les messages sur internet, elle pourrait lire le message, or, s'il est chiffré, elle ne peut pas le lire.

Pour illustrer ce qui vient d'être expliqué, le chiffrement de César qui a été utilisé dans l'escape game est un exemple parfait.

Si une personne veut envoyer un message à son ami sans que personne ne puisse le lire s'il intercepte le petit mot, les deux personnes communiquant peuvent se mettre d'accord sur un chiffrement.

Par exemple, s'ils se mettent d'accord sur un décalage de 1, comme dans l'exemple donné dans le jeu. Alors, pour envoyer salut, mon algorithme, c'est-à-dire mes étapes à suivre sont de remplacer chaque lettre par sa lettre correspondante selon le décalage.

SALUT devient alors TBMVU, comme l'illustration suivante.



Empreinte numérique, ou trace numérique

Les traces numériques d'une personne représente toutes les traces qu'elle a laissées sur internet. Cela peut être un compte, une photo, un message sur un forum, un like sur facebook, n'importe quel commentaire ou retweet.

Cela peut paraître anodin mais la plupart des gens n'ont pas conscience du volume de données que cela peut représenter et des conséquences possibles. Par exemple, une vieille photo de profil peut être vue par un employeur, votre identité peut être retrouvée, volée, ou encore, tous les systèmes de recommandation peuvent se nourrir de ces informations et orienter ce qui vous est proposé sur internet.

Les conséquences sont en fait très vastes, et ce, dans beaucoup de domaines ; éthique, législatif, numérique, etc…

Avoir conscience de cela permet ainsi de maîtriser ce que l'on appelle **l'identité numérique**, c'est-à-dire l'image de nous qui est reflétée sur internet, ou encore, la e-Réputation.

Pour plus d'informations vous pouvez consulter : https://www.childfocus.be/fr/prevention/securite-en-ligne/professionnels/les-reseaux-sociaux/empreinte-numerique-identite

Mots de passe et sa complexité

Auparavant, les mots de passe ne demandaient pas de complexité particulière. Aujourd'hui, des systèmes permettent à des hackers de trouver beaucoup plus facilement le moyen d'accéder aux comptes, par exemple en essayant les mots de passe les plus utilisés comme 123456789 ou azerty, ou encore, en utilisant des logiciels qui testent tous les mots de passe possibles. Pour se protéger, le meilleur moyen est encore d'utiliser des mots de passe très longs et/ou complexes.

La notion de bonne pratique dans le domaine peut différer quelque peu selon les experts, mais l'important est d'utiliser des mots de passe assez longs et de ne pas utiliser le même pour tous vos comptes afin d'éviter que votre mot de passe, s'il est trouvé, permette d'accéder à la totalité de votre réseau.

Phishing

Le phishing, ou hameçonnage est une technique qui consiste à usurper une identité pour obtenir des informations.

Par exemple, créer un faux site web sur lequel vous allez essayer de vous connecter permet de récupérer vos identifiants pour ainsi se connecter sur le vrai site. Vous envoyer un mail sous le nom d'une entreprise fiable pourrait vous pousser à cliquer sur un lien malveillant.

Ces techniques sont de plus en plus perfectionnées, et pour s'en protéger, plusieurs pratiques existent ;

- Vérifier l'adresse mail envoyant des mails
- Vérifier l'URL du site sur lequel vous naviguez (!! parfois le lien dans le mail semble correct mais vous dirige sur un site totalement différent !!)
- Avoir un antimalware installé sur votre ordinateur

Récupération

L'escape game proposé contient une étape consistant en une récupération d'informations sur un ordinateur. Ceci est en réalité possible grâce à l'utilisation de logiciels particuliers.

Il repose sur une particularité d'un élément qui se trouvent dans la plupart de nos ordinateurs ; les disques durs.

En effet, toutes nos données stockées dessus sont stockées *physiquement*. Dès lors, lorsque l'on « supprime » un fichier, en réalité, on dit à l'ordinateur qu'à l'avenir, il pourra mettre autre chose à la place.

En quelque mots, cela signifie que s'il on a vidé la corbeille un peu précipitamment, on peut toujours retrouver nos fichiers enfouis dans l'ordinateur, mais également que vider les fichiers pour vendre un ordinateur n'est pas suffisant pour tout faire disparaître…

Sauvegarde de sécurité/backup

Les sauvegardes de sécurité peuvent prendre diverses formes. L'objectif est de pouvoir retrouver des fichiers même en cas de problème sur votre ordinateur ou tout autre appareil.
Vous pouvez, par exemple ;

- Copier vos dossiers sur une clé usb, une carte sd, un disque dur, ou un autre ordinateur
- Placer vos dossiers sur un cloud

La technique ne doit pas être un frein à vos sauvegardes : n'hésitez surtout pas à faire des copies pour ne pas regretter de ne pas l'avoir fait plus tôt, peu importe où et comment.

Virus

Le virus est un type de malware. Le malware désigne, de manière générale, un logiciel malveillant placé sur un appareil.

Le virus a comme particularité de se « reproduire » et de pouvoir être partagé entre les ordinateurs en se propageant de fichier en fichier. Il peut avoir de nombreux effets, plus ou moins graves, et servent principalement à chiffrer ou voler des données sensibles, espionner un utilisateur, ou encore, rendre l'appareil inutilisable.

Contact

Elise Hallaert
elisehallaert@gmail.com
0489/158.692