



UNIVERSITÉ
CÔTE D'AZUR



MASTER
INFORMATIQUE

RAPPORT DE PROJET

Escape-game mobile sensibilisation à la cybersécurité

Réalisé par
Ossama ASHRAF
Ralph EL CHALFOUN
Jérémy HIRTH DAUMAS

Encadré par
Florian Ecard

Master Informatique
à Université Côte d'Azur
Deuxième semestre de l'année 2020-2021

Remerciement

Nous tenons tout particulièrement à remercier Monsieur Florian ECARD, notre encadrant, pour l'attention, le temps et la confiance qu'il a apportés à nous et notre travail, il nous a été d'un grande aide tout au long du processus de recherche et de développement de notre projet.

Table des matières

1	2
1.1	2
1.2	2
1.3	3
2	4
2.1	4
2.2	4
2.3	5
2.4	5
2.5	6
2.6	7
2.7	8
3	9
4	12
4.1	12
4.2	15
5	16
5.1	16
5.2	16
5.3	16
6	17
7	18
8	19

1 Introduction

1.1 Présentation du groupe

Notre groupe est composé de 3 membres : Ralph EL CHALFOUN, Jérémy HIRTH DAUMAS et Ossama ASHRAF. Nous sommes actuellement en première année de Master Informatique à l'Université Côte d'Azur.

Nous avons choisi de réaliser ce sujet de TER car il est orienté vers la sécurité informatique et les escape-games, deux notions qui nous intéressent particulièrement. L'aspect créativité nous a également motivé à participer à sa réalisation.

1.2 Présentation du projet

Depuis plusieurs années avec l'émergence des nouvelles technologies tels que l'informatique ou les réseaux, les cyberattaques sont de plus en plus présentes dans notre quotidien.

Celles-ci touchent à la fois des particuliers, des entreprises et parfois même des bâtiments essentiels comme les hôpitaux. Ceci est d'autant plus le cas en pleine crise pandémique de Covid-19, où des hôpitaux se voient bloqués l'accès à leurs propres machines informatiques en échange d'une rançon, provoquant ainsi de grave problème sur la réception et le traitement des patients.

D'après l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) (Source n°1 : [18](#)), la grande majorité des cyberattaques utilise la technique du phishing (hameçonnage en français), qui consiste à récupérer des informations personnelles sur la victime. Vient ensuite les ransomwares (rançongiciels en français) qui consiste à chiffrer toutes les données d'une machine en échange d'une rançon payée, souvent en crypto monnaie.

Selon un rapport publié par IBM Security en 2015 (Source n°2 : [18](#)), 60% des attaques informatiques ayant visé des entreprises en 2015 ont été initiées par quelqu'un de confiance. Parmi ce pourcentage, une partie a été effectuée par malveillance, c'est-à-dire volontairement. Mais la grande majorité des attaques internes reste due à une négligence de la part des employés, par exemple en accrochant un post-it sur un poste de travail contenant son mot de passe, ou bien télécharger des documents provenant de mails douteux.

Ces négligences peuvent se comprendre car les vecteurs d'entrées des cyberattaques sont bien souvent méconnus des employés. Une solution pour éviter de telles négligences serait de sensibiliser et former le personnel des entreprises à la cybersécurité, ainsi qu'à ses enjeux. Si cette sensibilisation pouvait être prise comme un jeu, c'est-à-dire avec des objectifs à accomplir en s'amusant, cela deviendrait plus entretenant et intéressant pour les employés.

C'est pourquoi un "escape-game" ayant des défis orientés cybersécurité conviendrait tout à fait à la situation. Pour rappel, un escape-game est un jeu d'énigmes qui se vit en équipe et où les joueurs doivent résoudre une série de casse-têtes dans un temps imparti pour accomplir une mission, ou bien s'échapper d'une pièce.

Cela permettrait aux employeurs de proposer de sensibiliser leurs employés à la cybersécurité tout en proposant une activité de "team-building", puisque ces challenges se résolvent en équipe.

1.3 Mise en place de l'escape-game

Pour la réalisation de cet escape-game nous avons décidé de tout d'abord chercher les vulnérabilités les plus fréquentes, en entreprise comme au quotidien. Après quelques recherches et par acquis d'expérience, nous avons réalisé un brainstorming avec l'aide de notre encadrant, et sommes arrivés à plusieurs notions. De ces notions nous voulons élaborer des challenges, visant chacun à faire réagir les joueurs quant à l'une des vulnérabilités les plus communes.

Deux choix se sont ensuite offerts à nous, les joueurs doivent-ils être du côté attaquant ou victime de la cyber-attaque ?

Nous nous sommes dit que positionner les joueurs en tant qu'attaquant serait la meilleure option. En effet, en leur proposant des challenges simples mais réels et en leur montrant des attaques simples, les participants comprendront certainement mieux les vulnérabilités dont ils pourraient être victimes quotidiennement. Et sachant que les futurs joueurs ne sont pas tous du domaine de la sécurité informatique, réussir ces différentes attaques les fera réagir sur le fait que c'est à la portée de tout le monde. Notre but sera ensuite de leur donner des conseils sur comment éviter au mieux ces attaques.

Après avoir identifié ces différentes notions, nous avons réalisé un challenge pour chacune d'entre elles. Les points ci-dessous démontrent notre approche.

2 La recherche et l'élaboration des challenges

2.1 Les cartes NFC

L'idée de ce challenge nous est venue grâce aux différents badges ou cartes NFC que nous possérons tous, ceux-ci permettent de déverrouiller une porte ou bien d'effectuer un paiement (badge de parking, carte étudiant, carte bancaire). Lors de cette épreuve, les candidats auront pour objectif de déverrouiller une serrure NFC, à l'aide d'une carte qu'ils devront cloner. La carte d'origine se trouvera quelque part dans la salle, fixée (ne pouvant être déplacée). On peut imaginer que la carte sera dans une pochette représentant la poche arrière du pantalon d'une personne en train de marcher.

Pour réaliser ceci nous nous sommes procuré une serrure NFC (avec cartes comprises) (Annexe n°1-2 : [19](#)) ainsi qu'un dispositif de lecture/écriture de carte NFC fonctionnant avec un ordinateur (Annexe n°3 : [20](#)). Initialement nous avons pensé au fait que les candidats pourraient utiliser ce lecteur/copieur pour réaliser le clonage de la carte. Mais après plusieurs tests de notre part nous nous sommes rendu compte que notre copieur de carte ne pouvait pas copier le secteur 0 des cartes (i.e. l'UID de la carte), également les cartes fournies avec la serrure NFC n'ont pas de secteur 0 reprogrammable. Or notre serrure NFC fonctionne par vérification de l'UID de la carte, alors si nous voulons être capable de copier la carte d'origine pour avoir deux cartes fonctionnelles, il nous faut obligatoirement copier l'UID de celle-ci. Après de multiples recherches, nous nous sommes orientés vers des cartes NFC Mifare Classic, qui ont la particularité d'avoir leur UID copiable et reprogrammable via un smartphone Android avec l'application MCT Android. Nous avons réalisé plusieurs tests avec nos smartphones Android qui se sont tous révélés concluants.

De plus, l'utilisation d'un téléphone pour effectuer la copie est plus intuitive que notre copieur d'origine, donc plus adapté pour des candidats débutants.

Les joueurs devront donc cloner la carte d'origine vers une carte vierge via l'application MCT Android (la carte vierge et le smartphone seront fournis aux candidats). Pour réaliser le clonage, un tutoriel leur sera fourni après avoir complété un autre challenge (Annexe n°4-5-6 : [20](#)).

À travers ce challenge, nous voulons faire prendre conscience aux utilisateurs de l'escape-game que, bien que la technologie nous facilite la vie au quotidien, elle peut représenter un réel danger. Notamment car ce procédé est facilement clonable si nous n'utilisons pas de pochette anti RFID/NFC pour ranger notre badge ou notre carte.

2.2 Le crochetage de cadenas

La sécurité informatique concerne la sécurité logicielle mais aussi matérielle. La sécurité physique est un aspect fondamental de la sécurité car elle participe à garantir l'intégrité, la confidentialité et la disponibilité des informations. Si quelqu'un réussit à accéder au système informatique de l'entreprise, il peut l'endommager ou même le détruire.

La sécurité physique consiste aussi en l'usage de barrières, alarmes, serrures et autres contrôles physiques permettant de conditionner l'accès physique aux locaux, aux ordinateurs et aux équipements. Ces mesures sont nécessaires pour protéger les ordinateurs, leur contenu et les autres ressources matérielles contre l'espionnage, le vol et la destruction accidentelle ou intentionnelle.

Forts de ce constat, nous avons décidé de créer un challenge qui porte sur ce thème. Ce challenge consiste à crocheter un cadenas. Le principe de crochetage est simple, il suffit d'aligner les goupilles qui sont à l'intérieur du cadenas grâce à un crochet et à un entraîneur. À l'aide d'un kit de crochetage, nous avons donc testé nous-même de crocheter un cadenas d'entraînement transparent. En moyenne, la première ouverture de ce type de cadenas nécessite deux à trois minutes. Dans le cas où les participants ne réussissent pas à déverrouiller le cadenas d'eux-mêmes, nous avons préparé un guide complet de crochetage (Annexe n°7-8 : 22). Les participants auront donc accès au kit et au guide. Le but de ce challenge est de sensibiliser les participants qu'un cadenas peut facilement être croché et qu'il faut utiliser des cadenas dont le crochetage est très difficile (cadenas avec des goupilles anti-crochetage ou avec de bonnes clés) voir des cadenas à code (Source n°3 : 18).

2.3 Les QR codes

Avec la crise sanitaire, le système du QR code est de plus en plus utilisé, notamment dans le domaine de la restauration (pour fournir une carte directement sur le smartphone du client). Nous les retrouvons également dans les applications, sur les emballages, dans les magazines, sur les parcmètres, ... Ces code-barres carrés peuvent contenir divers types d'informations, comme des URL, des mots de passe ou bien encore des numéros de téléphone. Les code-barres présentent ainsi un moyen simple et efficace pour un hacker puisqu'il peut par exemple injecter une url qui dirige vers un site malveillant. Pour ces raisons, nous avons décidé de faire un challenge portant sur ce thème.

Ce challenge consiste donc à scanner tout simplement un QR code qui a été préalablement assemblé lors du challenge “QR code” et qui va diriger les participants vers un site malveillant <https://hackernicois.herokuapp.com/> (Annexe n°9 : 23).

Le but ici est de sensibiliser les participants sur le fait qu'un QR code peut être conçu pour proposer un lien vers du contenu malveillant (sites internet qui usurpe l'identité d'un autre site “phishing”, sites internet faisant télécharger des malwares ou qui proposent du contenu illicite, etc.). Les hackers profitent du fait que la plupart des utilisateurs font aveuglément confiance au QR code. Il faut donc être vigilant lors du scan afin de ne pas être la victime d'un de ces QR code malveillants. Pour cela il faut avoir du bon sens et adopter les bonnes pratiques. Par exemple, il faut toujours bien vérifier l'url avant d'accéder au site, et vérifier qu'aucun autre QR code n'a été superposé dessus ... (Source n°4 : 18). Un malus sera accordé aux participants ayant scanné puis accédé au site via ce QR code malveillant.

2.4 Les macros

Le but de ce challenge est de sensibiliser les employés aux moyens de défense contre les macros office (Word/Excel) et aux risques que celles-ci peuvent engendrer si elles sont activées. Ces macros sont encore aujourd'hui un réel vecteur d'attaque car, selon une étude de Cofense Intelligence en 2018, près de 45% des logiciels malveillants sont distribués via des macros Microsoft Office (Source n°5 : 18). Parallèlement, selon une enquête de AlarmTILT, 72% des intrusions sont liées à des e-mails frauduleux reçus par le personnel (Source n°6 : 18). Ces deux chiffres montrent l'importance d'avoir un personnel sensibilisé aux risques liés aux macros (principalement envoyées par e-mail) et qui est capable de s'en protéger.

Les participants démarreront ce challenge lorsqu'ils trouveront la mauvaise clé USB (la clé USB violette) qu'ils voudront naturellement insérer dans l'ordinateur mis à disposition. Dans cette clé USB se trouvera un fichier Word nommé Indice.docm qui contiendra la phrase suivante « Pour visualiser l'indice veuillez activer les macros » et des images d'élément non chargé. Ce fichier contiendra également une macro office codée en VBA, qui, à l'activation, fera apparaître plusieurs "messagebox". Ceci aura pour but de déranger l'utilisateur avec "des messages" prévenant des risques d'insérer des clés USB d'origine inconnue, pouvant contenir des macros. Lorsque la personne ouvre le fichier elle aura la possibilité d'activer ou non les macros, si elle les active elle aura alors un malus, car elle aura fait preuve de négligence. Inversement si elle ne les active pas elle aura donc un bonus.

Quelque part d'autre se trouvera une bonne clé USB, celle-ci contiendra alors une énigme pour fournir un code (qui sera utile pour la suite) (Annexe n°10 : [23](#)), le but étant de ne pas fournir cette clé dès le départ pour inciter les joueurs à insérer la mauvaise d'abord.

2.5 Les mots de passe

Une notion primordiale dans la sécurité informatique réside dans la robustesse des mots de passe, surtout en ce qui concerne les comptes utilisateurs. Ces comptes peuvent donner accès à des données basiques (par exemple un forum) ou fournir à un attaquant des données plus sensibles, telles que des informations bancaires ou personnelles. Cela peut engendrer par la suite un risque direct envers l'utilisateur ou l'organisation concernée (entreprise). Un escape-game sensibilisant à la cybersécurité n'abordant pas ce thème nous paraît peu représentatif de la réalité, nous avons donc mis en place un challenge sur cette notion.

Microsoft Digital Defense (Source n°7 : [18](#)) détaille les principales menaces auxquelles les entreprises sont confrontées et environ 80% des failles de sécurité proviennent d'un vol d'identifiants, presque 73% des mots de passe sont dupliqués sur plusieurs services, enfin 80% des employés utilisent des applications non approuvées (les applications customisées ou non vérifiées sont créées par les développeurs pour des usages exclusifs au sein d'entreprises, comme une application de gestion de clients ou afin d'être téléchargées directement depuis Internet).

Pour ce challenge, les candidats tenteront de deviner un mot de passe utilisateur, ce mot de passe sera basique. Pour cela nous avons besoin d'une plateforme sur laquelle créer un compte. Nous avons donc réalisé un pseudo site-vitrine pour notre escape-game.

Le site se base sur du PHP-HTML, Javascript ainsi que MongoDB. Il devra ensuite pouvoir être accessible de partout afin de rester sur un escape-game mobile. Nous choisissons donc de faire appel à la plateforme HEROKU afin de mettre en ligne ce site. La partie PHP nous permet à la fois de déployer le site sur HEROKU mais également de gérer les connexions/sessions utilisateurs ce qui est parfait pour ce challenge. Tout en voulant rester dans l'optique "Mobile" nous ne voulions pas coder en "dur" la partie connexion donc il fallait stocker le compte utilisateur à "hacker" quelque part autre que dans le code, et c'est ici que MongoDB nous est utile.

MongoDB est une base de données NoSQL qui permet de nous connecter à notre base via un Cluster MongoDB créé spécialement pour ce TER. Grâce à quelques modifications d'accessibilités via le site MongoDB Atlas, nous pouvons y accéder de n'importe où.

Dans de futurs tests, nous nous sommes rendu compte que l'affichage du site sur smartphone n'était pas adapté, nous avons donc réalisé une refonte graphique (CSS) afin qu'il soit agréable à utiliser/lire sous format mobile (Annexe n°11 : [24](#)).

Une fois les fondations construites, c'est-à-dire un site avec un système de "login" accessible depuis Internet, il nous fallait un compte à "hacker".

Les erreurs les plus courantes dans le choix d'un mot de passe sont de le rendre court et devinable. Par devinable, nous entendons le fait de pouvoir deviner le mot passe grâce à des informations visibles de tout le monde en cherchant un peu sur internet, ou en connaissant la personne. Afin d'aider les joueurs, nous avons choisi de leur fournir un document basique où se trouve un grand nombre d'informations : un Curriculum Vitae. Grâce à ce CV, les candidats auront dans un premier temps accès à l'email de l'employé à hacker, soit le premier élément d'une connexion à un compte. Et dans un second temps il faut trouver le mot de passe de cette personne.

Nous avons tout d'abord pensé à mettre "prénom-numéroDeDépartement" comme mot de passe, ce qui donnerait "Alexandre06" (Alexandre étant le prénom de notre faux employé à qui le CV appartient). Mais après quelques tests entre nous et des amis, nous nous sommes rendu compte que cela prendrait plus de temps que prévu pour trouver le mot de passe, (bien qu'il finisse en général par être découvert). Afin que notre escape-game reste court en termes de temps, il nous a fallu choisir un autre mot de passe.

Pour cela et afin qu'il soit plus facilement devinable nous devons insister sur le thème de ce mot de passe. Nous prenons finalement le thème du voyage, notre faux employé est un passionné de voyage et en particulier des voyages au Canada. Par la répétition du mot Canada et de ses expériences de travail là-bas, nous espérons que les joueurs saisiront le message et réussiront à trouver le mot de passe qui sera simplement "Canada". Nous avons donc réalisé d'autres tests, et les résultats étaient assez satisfaisants, nous avons donc décidé de le garder (Annexe n°12 : [25](#)).

Ce problème est comme dit précédemment très fréquent et pour y remédier il est indispensable de choisir correctement son mot de passe, soit un long mot de passe, n'ayant pas sens en particulier afin de réduire les chances de deviner le mot de passe grâce à des informations trouvées sur le net ou autre. De plus, il faut éviter de choisir le même mot de passe pour plusieurs comptes car une application non approuvée ou peu sécurisée risque de facilement faire fuiter sa base de données, voire de vendre les données personnelles incluant les mots de passe. Ce qui engendrera la faiblesse de tous les autres comptes utilisant le même mot de passe. Enfin, pour encore plus de sécurité, il faudrait changer régulièrement de mots de passe, une fois tous les 6 mois est raisonnable, surtout pour les comptes sensibles/importants. Seulement 36% des entreprises, de moins de 50 employés, changent les mots de passe de leurs ordinateurs de bureau au moins tous les 6 mois selon une étude de CPME (Source n°8 : [18](#)).

2.6 Les autres erreurs communes

Dans une entreprise, il est fréquent de trouver les mots de passe des sessions Windows/Mac/Linux écrits directement sur un post-it. Parfois caché sous un clavier, ou même directement collé sur le moniteur. Bien que cela se fasse de moins en moins, il est essentiel de le rappeler. Ceci est un exemple d'erreur basique parmi d'autres, afin donc de compléter au mieux notre projet, nous avons réalisé des mini-challenges pour y faire référence.

Dans la pièce de l'escape-game se trouvera un ordinateur à disposition des candidats, mais celui-ci sera verrouillé. Le code d'accès se trouve sur un post-it collé sous le clavier de l'ordinateur. L'objectif des participants sera de trouver ce post-it afin de pouvoir se connecter sur la machine (rien de vraiment difficile). Une fois connectés sur l'ordinateur, si les participants ont la bonne idée de vérifier dans la corbeille de celui-ci, ils trouveront un document bonus sur les bonnes pratiques à adopter lorsque l'on scanne un QR code (Annexe n°13 : [26](#)). Également dans la salle, se trouvera une broyeuse à papier, cette dernière découpe, en lamelle fine uniquement (coupe droite), ce que nous y insérons (Annexe n°14 : [26](#)). Un papier déjà découpé s'y trouvera, les joueurs devront tenter de le reconstituer afin d'en lire son contenu. Afin de faciliter sa lecture, nous y avons inséré des courbes en background, et le texte inscrit sera écrit en grande taille (Annexe n°15 : [27](#)).

Ces énigmes feront comprendre aux candidats l'importance de ne pas marquer leurs mots de passe sur un bout de papier car celui-ci peut tomber entre de mauvaises mains. Puis que lorsqu'on supprime un fichier, ce dernier n'est pas réellement supprimé. Via l'ordinateur, il sera disponible dans la corbeille et quand bien même le fichier est supprimé de cette dernière, il peut toujours être présent dans l'ordinateur. Une solution pour être sûr de sa suppression serait d'utiliser un logiciel destructeur de fichier. Et via une broyeuse, il faut privilégier une coupe croisée, voire une micro-coupe, afin de compliquer la reconstitution du document (Annexe n°16 : [27](#)).

2.7 Donner une finalité à l'escape-game

Pour compléter finalement tous les challenges et donner une finalité à l'escape-game nous avons pensé attribuer une sorte de "note" sur la performance de l'équipe qui a participé. Cette note aura pour but à la fois de s'auto évaluer mais également de permettre aux différentes équipes d'une entreprise de comparer leurs résultats, d'en discuter et de faire peut-être réagir les employés et/ou l'entreprise. Ce système d'évaluation est évidemment donné à titre indicatif car nous ne sommes pas des experts de la cybersécurité et nous ne pouvons réellement juger la sécurité d'une entreprise par une performance de jeu. C'est pourquoi nous orienterons cette évaluation finale vers des conseils/rappels.

Nous devons maintenant trouver un moyen d'évaluer et nous avons pensé réaliser un sondage où nous pouvons à la fois recueillir les avis des joueurs sur l'escape-game et à la fois leur poser des questions sur leurs habitudes en termes de sécurité informatique.

D'abord basiquement, nous leur demanderons pour chaque challenge s'ils ont réussi ou non, ensuite nous leurs poseront diverses questions telles que leurs fréquences de changement de mot de passe, utilisent-ils un système Anti-RFID pour protéger leurs cartes sans contact, ... (Annexe n°17 : [28](#)) Enfin, ils auront à disposition une zone de texte, leur permettant de laisser des commentaires sur les challenges, ou leur avis global de l'escape-game (Annexe n°18 : [28](#)).

Toujours dans l'optique de garder la notion mobile de l'escape-game, nous avons choisi d'introduire ce sondage dans notre site vitrine, ainsi les réponses des équipes pourront y être stockées.

Grâce à ces résultats, nous pourrons à l'avenir modifier certaines épreuves, en ajouter ou en enlever, en fonction des réponses, afin de cibler au mieux les erreurs les plus fréquentes.

3 Réalisation du scénario

Une fois nos idées de challenges trouvées, il nous fallait les assembler pour réaliser un scénario d'escape-game.

Si l'on essaye d'associer toutes nos idées, nous nous rendons rapidement compte que beaucoup de nos challenges sont basés sur le principe de déverrouiller quelque chose. Nous avons déjà un cadenas à crocheter ainsi qu'un cadenas NFC. Le challenge de la broyeuse ainsi que celui de la clé USB peuvent fournir un code ou un message.

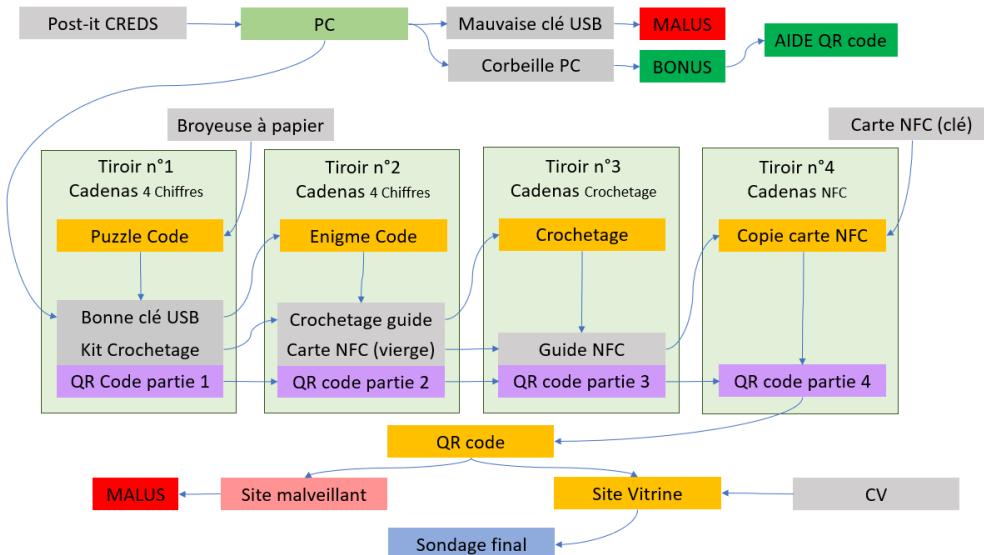
C'est ici que nous avons eu l'idée d'utiliser une petite commode à plusieurs tiroirs pour ainsi centraliser l'escape-game (Annexe n°19 : [29](#)). Ces tiroirs seront verrouillés par différents cadenas. Cependant ces tiroirs ne peuvent rester vides, il nous fallait dissimuler quelque chose à l'intérieur.

Nous trouvions que l'énigme du QR code à scanner était assez simple, et avons donc décidé de couper le QR code en 4, afin de répartir ces morceaux dans les différents tiroirs (Annexe n°20 : [29](#)).

Rappelons que cette énigme du QR code redirige vers deux adresses différentes, une bonne et une mauvaise, les deux sites précédemment créés sont la suite parfaite de ce challenge. Une fois le bon site trouvé c'est-à-dire le site vitrine, les candidats devront passer le challenge où il faut trouver le mot de passe grâce au CV et par la suite ils pourront accéder au sondage de fin et donc terminer l'escape-game.

En partant de cette idée, nous avons donc choisi d'illustrer le déroulement à l'aide d'un puzzle flow.

Voici ce qui a été réalisé :



En lisant ce puzzle flow d'en haut à gauche vers en bas à droite, nous pouvons expliquer le scénario de cette façon :

- ▶ Les joueurs commenceront soit par déverrouiller le PC grâce aux données écrites sur le POST-IT soit par déchiffrer le code dans la broyeuse à papier (fournissant le code du 1er Tiroir).
- ▶ Parallèlement ils auront dès le début à disposition la mauvaise clé USB. S'ils insèrent cette dernière dans le PC et qu'ils ouvrent et activent les macros du fichier présent à l'intérieur, ils obtiendront un Malus pour le score final.
- ▶ De même une corbeille est présente sur le bureau virtuel du PC, avec à l'intérieur un fichier, si ce dernier est ouvert, il donnera un Bonus pour le score final.
- ▶ Une fois le premier tiroir déverrouillé, les joueurs obtiendront la première partie du QR code, ainsi qu'un kit de crochetterie et la bonne clé USB.
- ▶ A partir de là deux choix s'offrent aux candidats :
 - Lire le contenu de la nouvelle clé USB
 - Tenter d'ouvrir le cadenas à crocheter grâce au KIT
- ▶ Dans le premier cas, ils découvriront une énigme, qui une fois résolue leur donnera le code à 4 chiffres pour le cadenas du deuxième tiroir, une fois ouvert ils obtiendront la deuxième partie du QR code ainsi qu'un guide de crochetterie (utile pour le troisième tiroir), et enfin une carte vierge NFC.
- ▶ Dans le deuxième cas, c'est le cadenas du troisième tiroir qu'ils déverrouilleront, et ils obtiendront un guide de copie-NFC ainsi que la troisième partie du QR code. Ce troisième tiroir peut être difficile à déverrouiller c'est pourquoi le guide du deuxième tiroir est souvent requis.
- ▶ A ce stade il ne reste qu'un seul tiroir, le quatrième. Celui-ci est le plus complexe et nécessite obligatoirement l'ouverture du deuxième tiroir afin d'avoir la carte NFC vierge, et de préférence le guide obtenu dans le troisième. Grâce à ces éléments ainsi qu'un smartphone Android fournis, les joueurs pourront copier la carte NFC placée sur la commode (cette carte permet d'ouvrir le cadenas NFC, mais cette dernière est fixée, donc impossible à utiliser en l'état) et ainsi déverrouiller l'ultime tiroir. Ils obtiendront enfin la dernière partie du QR code.

- Désormais en possession des 4 parties, ils ne leurs restent donc qu'à assembler les morceaux pour former le QR code et à en scanner les deux faces, ici ils devront faire attention à l'url vers laquelle redirige le scan car :
 - Une face redirige vers un site "malveillant" leur faisant obtenir un malus
 - L'autre face redirige vers le site-vitrine de l'escape-game, plus précisément sur l'interface de connexion.
- Une fois sur le bon site, les joueurs sont face au dernier challenge qui est de trouver le mot de passe et l'email de l'utilisateur afin de se connecter sur son profil. Depuis le début, un CV est mis à disposition sur le bureau à côté du PC. Grâce à ce dernier, les joueurs devront réussir à trouver les identifiants et hacker le compte du faux employé.
- Après cela, ils auront terminé l'escape-game, et seront redirigés vers le sondage final, contenant les différentes questions quant aux habitudes des joueurs. Ils pourront également cocher les malus et bonus obtenus, et enfin obtenir leur score.
- Dans le cas où les joueurs n'auraient pas réussi à accéder au sondage dans le temps imparti, nous prévoyons de les rediriger directement vers ce dernier pour qu'ils puissent quand même y répondre.

4 Test

Notre prototype d'escape-game ainsi terminé, nous passons donc à la phase de test. Pour cela nous avons essayé au mieux de nous mettre dans des conditions réelles, malheureusement nous n'avons pas pu proposer l'expérience à un groupe de personnes étrangères au projet. Cependant d'autres tests pourront être effectués par l'entourage de notre encadrant Florian ECARD et pour lui faciliter la tâche nous lui avons réaliser une fiche de test répertoriant toutes les épreuves afin d'y noter le temps passé sur chaque challenges (ce que le sondage ne prend pas en compte) (Annexe n°21 : [30](#)). Nous en sommes donc arrivés au résultats suivants.

4.1 Les challenges

Pour chaque challenge, nous en avons chronométré la performance, et déterminé de façon arbitraire (vis-à-vis des attentes) la difficulté.

► Le post-it :

- Accès au challenge : 1-4 minutes, le post-it est collé sous le clavier, tout dépendra des habitudes des joueurs.
- Temps d'exécution : quasiment nul étant donné qu'il faut simplement entrer les données sur l'ordinateur.
- Difficulté : facile.
- Améliorations possible : coller simplement le post-it sur l'écran.

► La broyeuse à papier :

- Accès au challenge : si la pièce est vidée de tout autre meuble non en relation avec l'escape-game, le temps pour trouver ce challenge est d'environ 1 minute, autrement en fonction du nombre de meubles cela peut varier en augmentant.
- Temps : environ 4 minutes.
- Difficulté : moyenne, le principe est simple (reconstituer un puzzle) par contre l'exécution prend du temps.
- Améliorations possible : il faudrait simplifier d'avantage le puzzle (chiffres plus gros et plus visibles).

► La mauvaise clé USB :

- Accès au challenge : simple, la clé est mise à disposition près de l'ordinateur.
- Temps : environ 1-2 minutes, l'activation des macros a pour but de faire perdre du temps aux joueurs.
- Difficulté : moyenne, le but étant de ne pas activer les macros de cette clé, si les joueurs ne l'insèrent pas ou suivent les avertissements du logiciel de traitement de texte, ils réussiront facilement.
- Améliorations possible : donner plus envie aux joueurs d'insérer cette clé (trouver un meilleur moyen de la mettre en évidence).

► La corbeille du PC :

- Accès au challenge : difficile, les joueurs sont rarement bloqués au point de penser à vérifier la corbeille.
- Temps : quasi nul, une fois trouvé il suffit de lire le contenu du fichier.
- Difficulté : difficile, étant uniquement un bonus, la difficulté à trouver le document ne gêne pas au déroulement de l'escape-game.
- Améliorations possible : non nécessaire.

► La bonne clé USB :

- Accès au challenge : facile, les joueurs l'obtiennent dans le premier tiroir.
- Temps : 5 minutes, l'éénigme est complexe pour certaines personnes.
- Difficulté : difficile, si les joueurs ne sont pas fort en déduction et avec les nombres cela risque de prendre plus de temps que prévu.
- Améliorations possible : non nécessaire.

► Le crochetage de cadenas :

- Accès au challenge : facile lorsque les joueurs ont obtenu le guide.
- Temps : 5-7 minutes (le temps de lecture du guide et de crocheter le cadenas), les joueurs pourront cependant réaliser ce challenge en parallèle d'un autre.
- Difficulté : difficile, sans le guide le taux de réussite est très faible, avec le guide les joueurs finissent par réussir.
- Améliorations possible : avec un guide explicite et une vidéo, les améliorations sont difficiles à trouver.

► Le cadenas NFC :

- Accès au challenge : difficile, les joueurs ne savent pas à l'avance que le tiroir n°4 se dévrouille grâce à une carte NFC.
- Temps : 6-8 minutes (le temps de lecture du guide et de copier la carte), le challenge n'est pas évident à comprendre.
- Difficulté : très difficile, sans le guide c'est impossible à moins de l'avoir déjà réalisé. La manipulation entre les cartes et le téléphone n'est pas simple, c'est pour cela que nous avons mis cette épreuve pour le dernier tiroir.
- Améliorations possible : indiquer que le tiroir n°4 est à cadenas NFC. Malgré la simplification via l'utilisation d'une application smartphone, cette épreuve reste la plus complexe mais également la plus intéressante vis-à-vis de la cybersécurité. Il serait dommage de l'enlever. Nous pourrions donner plus d'indications sur le déroulé de l'épreuve, sans trop en dire afin que cela rester un challenge.

► Le scan des QR code :

- Accès au challenge : difficile, il faut rassembler les quatre morceaux de QR codes via les challenges précédent.
- Temps : 2 minutes, assemblage du QR code.
- Difficulté : indéterminée, les joueurs auront tout d'abord une chance sur deux de scanner le bon code en premier, et dans le cas contraire ils devront vérifier l'url avant d'accéder au site.
- Améliorations possible : simplifier le puzzle en ajoutant une couleur à chaque face du QR code (ex : un point vert sur chaque face du premier code, et un point bleu sur les faces de l'autre code). Pour rappel le contenu du document de la corbeille du PC indique de se méfier des QR code.

► Le CV/mot de passe :

- Accès au challenge : difficile car c'est l'une des dernières épreuves, mais le CV est mis à disposition sur le bureau depuis le début.
- Temps : 4 minutes, temps de lecture du CV + quelques tentatives de mot de passe.
- Difficulté : trouver le mot de passe via le CV est désormais simple, cependant savoir que nous recherchons les identifiant/mot de passe sur le CV rendent le challenge difficile.
- Améliorations possible : expliciter le fait que le mot de passe est sur ce CV (citer quelque part que nous cherchons à hacker le compte d'un dénommé Alexandre DU-BOIS, par exemple...).

► Le sondage :

- Accès au challenge : sachant que c'est le dernier, il est évidemment le plus difficile d'accès, mais la redirection directe (du challenge précédent à celui-ci) le rend autant difficile.
- Temps : 2 minutes, temps de remplissage du sondage.
- Difficulté : seule la partie "questions sur la cybersécurité" est considérée comme un challenge, le reste se remplit sans difficultés.
- Améliorations possible : ajouter/changer les questions régulièrement selon les scores obtenus afin de diversifier les statistiques.

4.2 L'ensemble de l'escape-game

Globalement, le temps d'exécution de tout l'escape-game varie entre 30 et 38 minutes. C'est plus que ce que nous désirions de base, à savoir environ 20 minutes. Cependant, nous en avons fait part à notre encadrant et il fut satisfait. Sachant que nous pouvons encore faire des améliorations, comme cités pour une grande partie des épreuves.

Au niveau de la difficulté des challenges, nous aimerais réduire le temps d'accès aux énigmes, sans pour autant simplifier l'accomplissement des challenges. Cela aura pour but de faire essayer un maximum d'épreuves aux joueurs et donc montrer le plus de notions possibles, car notre objectif est de sensibiliser les participants à la cybersécurité en plus de renforcer le "team-building" au sein de l'entreprise.

Nos attentes n'étaient donc pas éloignées de la réalité, quant au déroulement global. Nous devons notamment réaliser les améliorations citées et faire plus de tests afin de proposer une expérience plus riche aux joueurs.

5 Gestión del proyecto

5.1 La recherche des challenges

Pour ce qui est de la recherche des challenges, nous avons tous participé grâce au brainstorming avec notre encadrant, les idées sont venues très rapidement, nous laissant plus de temps pour l'élaboration.

5.2 L'élaboration des challenges

En suivant nos idées, nous nous sommes répartis les challenges comme cela :

- ▶ Ralph EL CHALFOUN : j'ai réalisé le site vitrine (challenge : mot de passe, sondage), ainsi que la confection des QR codes, de l'énigme des 2 cadenas à code, du guide NFC et enfin la confection du meuble final.
- ▶ Jérémy HIRTH DAUMAS : j'ai programmé le document pour le challenge des macros (mauvaise clé USB), également j'ai rédigé le faux CV (challenge mot de passe), enfin je me suis occupé de la réalisation du challenge des cartes NFC.
- ▶ Ossama ASHRAF : j'ai programmé le mauvais site, je me suis occupé de la réalisation de l'épreuve du crocheting du cadenas ainsi que de son guide, enfin j'ai créé le document de la corbeille du PC.

Malgré le fait que nos travaux sont différents, nous nous sommes aidés/consultés mutuellement au fil des semaines, afin de connaître les avis de chacun.

5.3 La communication et l'organisation

Afin de communiquer entre-nous, nous avons créé un serveur Discord avec différents channels pour chaque challenges/notions du projet. Pour l'écriture de ce rapport nous avons tous participé à sa rédaction grâce à un Google Doc, et nous avons ainsi pu le montrer en amont à notre encadrant qui nous a suggéré divers changements.

Pour la communication entre notre encadrant et nous, nous échangeons régulièrement des mails et avons environ un rendez-vous toutes les 2 semaines (appel vocal/rencontre physique).

6 Conclusion

En conclusion de ce projet de création d'escape-game mobile sur la sensibilisation à la cybersécurité, nous avons réussi à concevoir un prototype à la fois mobile et fonctionnel. Bien que les demandes de notre encadrant étaient précises, il nous a laissé une grande part d'improvisation, nous permettant d'être autonomes et créatifs. La combinaison d'un "brainstorming" et d'un puzzle flow nous a permis d'arriver à ce travail.

Nous avons tenté au mieux de réaliser des tests, qui nous ont déjà permis de déterminer les améliorations à venir, soit la modifications de certains challenges. Mais à chaque modification qu'il adviendra, nous devront de nouveau réaliser d'autres tests, c'est pourquoi nous avons mis en place le sondage et la fiche d'épreuves qui nous faciliteront cette tâche.

Nous avons rencontré, tout au long de la création, des problèmes tels que la technologie des premières cartes NFC qui n'étaient pas adaptés, le challenge du CV/mot de passe qui manquait d'explicitation, ou encore le site vitrine, dont la refonte graphique a été nécessaire pour l'adapter au format smartphone.

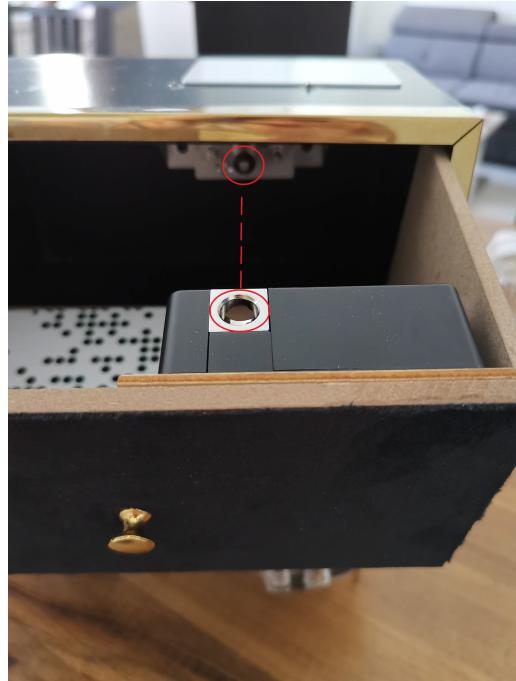
Enfin, ce projet qui a été conçu de A-Z nous a permis d'en apprendre plus sur la cybersécurité, a développé notre autonomie et notre créativité. Nous savons que le produit crée a encore besoin d'améliorations pour être effectif, c'est pourquoi nous espérons qu'il contribuera à l'objectif de notre encadrant et permettra aux futurs joueurs d'en apprendre également d'avantage sur les bonnes pratiques de la sécurité informatique.

7 Sources

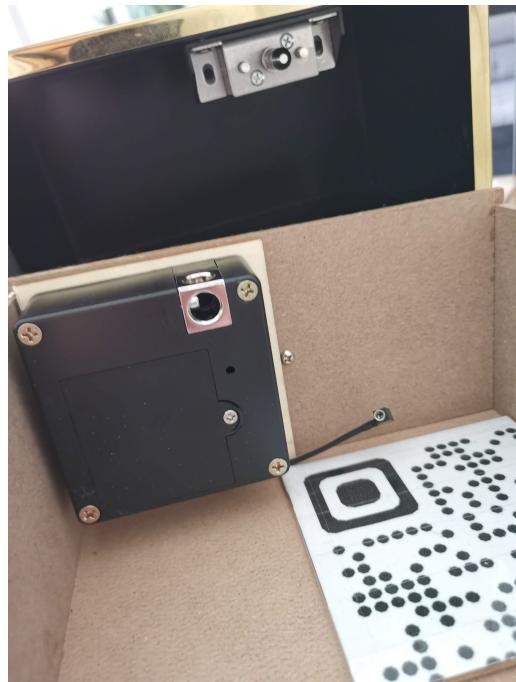
- (1) <https://www.ssi.gouv.fr/particulier/principales-menaces/cybercriminalite/attaque-par-hameconnage-phishing/>
- (2) <https://www.lesechos.fr/2016/06/la-plupart-des-cyberattaques-contre-les-entreprises-sont-dorigine-interne-208352>
- (3) <https://crocheteursdefrance.fr/2017/11/12/goupilles-anti-crochetages/>
- (4) <https://www.csionline.com/article/3584773/how-attackers-exploit-qr-codes-and-how-to-mitigate-the-risk.html>
- (5) <https://meterpreter.org/cofense-intelligence-45-of-malware-are-sent-via-microsoft-office-macros/>
- (6) <https://www.alarmtilt.com/fr/infographies/1268-la-cybersécurité-en-chiffre>
- (7) <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWxPuf>
- (8) <https://www.cpme.fr/positions/numerique/16-chiffres-cles-sur-la-cybersecurite-des-entreprises-50-salaries>

8 Annexes

Annexe 1 : Système de verrouillage par serrure NFC 1/2



Annexe 2 : Système de verrouillage par serrure NFC 2/2



Annexe 3 : Lecteur NFC



Annexe 4 : Tutoriel copie de carte NFC 1/3

Tutoriel de copie de carte NFC - 1/3

Rendez vous à l'aide d'un smartphone dans l'application MCT

N'oubliez pas d'activer la fonction NFC de votre smartphone

Positionnez la carte à copier au dos de votre smartphone en la déplaçant, jusqu'à obtenir un message en bas de l'écran (1).

Nous vous conseillons de poser le badge sur un plan dur puis de poser votre smartphone par dessus afin d'éviter tout faux mouvement.

Choisissez "Read Tag" (2).

Les 2 dictionnaires doivent être cochés (3).

Lancez la procédure de lecture (4).

Une fois la lecture terminée, sauvegardez le contenu (5).

Nommez votre fichier puis enregistrez le (6).

L'image de votre carte original ("Dump") est à présent enregistrée dans votre smartphone.

Annexe 5 : Tutoriel copie de carte NFC 2/3



N'oubliez pas d'activer la fonction NFC de votre smartphone

Positionnez votre badge vierge au dos de votre smartphone jusqu'à obtenir le message "New tag found" en bas de l'écran.

Choisissez "Write Tag" (7) puis "Write Dump" (8).

ATTENTION : VOUS DEVEZ COCHER LES 2 OPTIONS PROPOSÉES DANS "SHOW OPTIONS" (9).

Sans ces 2 mesures, l'UID ne sera pas copié et le badge NE SERA PLUS REINSCRIPTIBLE.

A chaque écriture, il vous faudra absolument cocher ces 2 options.

Choisissez le dump de votre badge original (10/11) puis validez (12).

Annexe 6 : Tutoriel copie de carte NFC 3/3



N'oubliez pas d'activer la fonction NFC de votre smartphone

Tous les secteurs doivent être cochés. Validez (13).

Les 2 dictionnaires doivent être cochés (14).

Lancez la procédure de copie (15).

Vous obtiendrez le message d'erreur "Error: Some error occurred while writing. This could be really bad" en bas de l'écran (16). Ce message est normal.

Les contrôleurs NFC présents dans les Smartphones étant peu performants, les échanges de données lors de l'écriture sont parfois difficiles.

Il vous faudra recommencer la procédure (à partir du numéro 10) jusqu'à obtenir le message de réussite "Data successfully written" en bas de l'écran (17).

La copie est à présent effectuée. Il ne vous reste plus qu'à l'utiliser !

Annexe 7 : Tutoriel de crochetage 1/2

Apprentissage du lock picking ou crochetage de serrure

Ce document explique les étapes à suivre pour crocheter une serrure.



Kit de crochetage



Il existe plusieurs crochets à disposition



Le plus facile à utiliser est celui-ci



Ensuite, il faut choisir un entraîneur

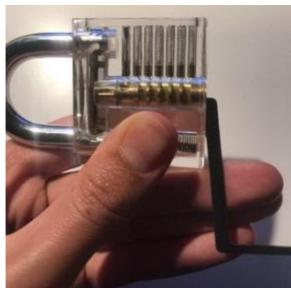
Annexe 8 : Tutoriel de crochetage 1/2



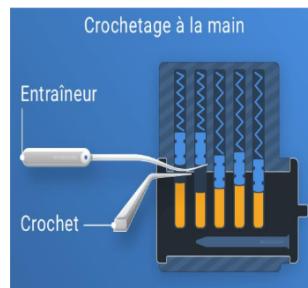
La première étape consiste à introduire l'entraîneur dans le cadenas comme dans l'image ci-dessous . Remarquez bien la pression exercée par les doigts sur l'entraîneur, elle est importante.



La deuxième et dernière étape consiste à utiliser le crochet pour aligner toutes les goupilles du cadenas (tout en gardant la pression des doigts sur l'entraîneur).



Voici le cadenas avec toutes ses goupilles bien alignées



À ce stade, il suffit de pousser l'entraîneur vers l'arrière pour ouvrir le cadenas.
Image illustrant le principe du crochetage.

Démonstration en vidéo : <https://youtu.be/ugA6UsvvYy0?t=226>

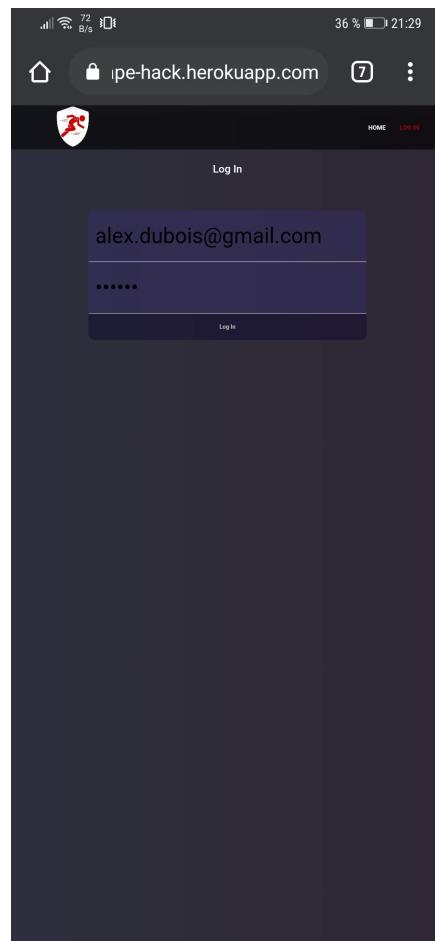
Annexe 9 : Capture d'écran du mauvais site Web "hacker"



Annexe 10 : Enigme pour révéler un code à 4 chiffres "3145"



Annexe 11 : Capture d'écran du système de log in sur le site vitrine



Annexe 12 : Document du Faux CV d'Alexandre DUBOIS

Alexandre DUBOIS

Développeur FULL-STACK



PROFIL

Passionné depuis mon enfance par le Canada où je partais régulièrement en vacances avec mes parents. Je suis resté attaché à ce pays et je recherche désormais un travail à Montréal pour y vivre définitivement.

 + 33 6 46 45 34 76
 alex.dubois@gmail.com
 Montréal, Canada
 Française

EXPÉRIENCES PROFESSIONNELLES

Google
Du 24/05/2017 au 18/02/2020 (Toronto-Canada)
Développeur Front-End
Tâches réalisées :

- Optimisation des fonctionnalités de la plateforme web.
- Anticipation et proactivité en matière de stratégie web corporate.
- Création d'outils IT intégrés dans la communication et dans la gestion RH internes.

Amadeus
Du 12/01/2016 au 21/03/2017 (Nice-France)
Développeur FULL-STACK
Tâches réalisées :

- Fonction généraliste dans la conception et le développement de sites web.
- Elaboration de projets au sein d'une équipe pluridisciplinaire en webmarketing.
- Implémentation de sites web responsive, optimisés pour l'univers mobile.

Monte-Carlo Société des Bains de Mer
Du 01/06/2015 au 10/12/2015 (Monaco)
Développeur FULL-STACK
Tâches réalisées :

- Fonction généraliste dans la conception et le développement de sites web.
- Elaboration de projets au sein d'une équipe pluridisciplinaire en webmarketing.
- Implémentation de sites web responsive, optimisés pour l'univers mobile.

FORMATION

2013-2015	Masteur Informatique
Nice-France	<i>Université Nice-Sophia-Antipolis</i>
2010-2013	Licence Informatique
Nice-France	<i>Université Nice-Sophia-Antipolis</i>

LOGICIELS

Excel	● ● ● ● ●
PowerPoint	● ● ● ● ●
Word	● ● ● ● ●

RÉSEAUX SOCIAUX

-  profil.skype
-  url.linkedin
-  profil.twitter
-  www.ILoveCanada.com

CENTRE D'INTÉRÊTS

- Voyager : Canada (Montréal, Toronto, Vancouver).
- Sport : Ski, natation, randonnée et golf.

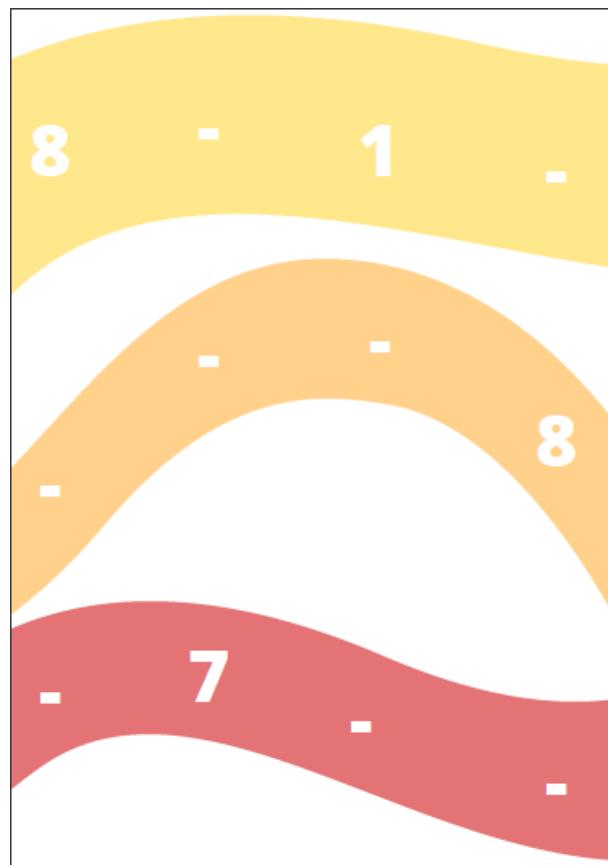
Annexe 13 : Document se trouvant dans la corbeille du PC



Annexe 14 : Enigme "puzzle" de reconstitution d'un document broyé en coupe droite



Annexe 15 : Document pour l'énigme de la broyeuse révélant le code "8718"



Annexe 16 : Image illustrant les différentes coupe (droite - croisée - micro)



Coupe droite



Coupe croisée



Micro coupe

Annexe 17 : Capture d'écran du sondage sur le site vitrine 1/2

The screenshot shows a mobile application interface for a survey. At the top, there are standard smartphone status icons (signal, battery, time). Below that is a header bar with a lock icon and the URL 'ipe-hack.herokuapp.com'. The main title 'Sondage' is centered above a red button. The first section is titled 'Informations' and contains a question 'De combien de personnes votre groupe est composé?' followed by a text input field containing 'Nom...'. The second section is titled 'Général' and contains several questions with toggle switches (on/off buttons):

- Possédez-vous des mots de passe comportant une information personnelle (date de naissance / prénoms) ? (On)
- Utilisez-vous un même mot de passe pour plusieurs comptes ? (On)
- Ennez-vous vos mots de passe quelque part sur un papier ou dans votre téléphone ? (On)
- Utilisez-vous un VPN lors d'une connexion sur réseau public ? (On)
- Protégez-vous vos carte NFC (carte sans contact) avec un système Anti-RFID ? (On)
- Utilisez-vous une "station blanche" (ordinateur caboyé déconnecté du réseau) pour tester la légitimité d'une clé USB ? (On)

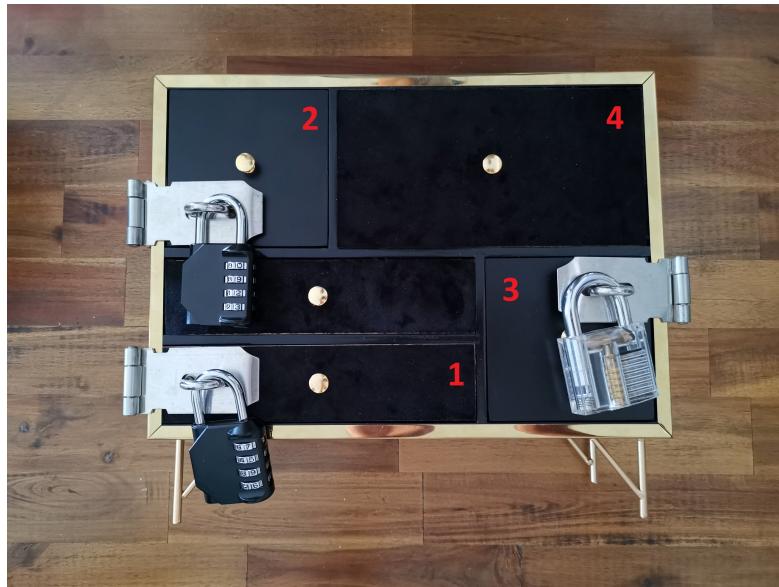
Annexe 18 : Capture d'écran du sondage sur le site vitrine 2/2

This is the second part of the survey from the previous screenshot. It starts with a list of challenges with toggle switches:

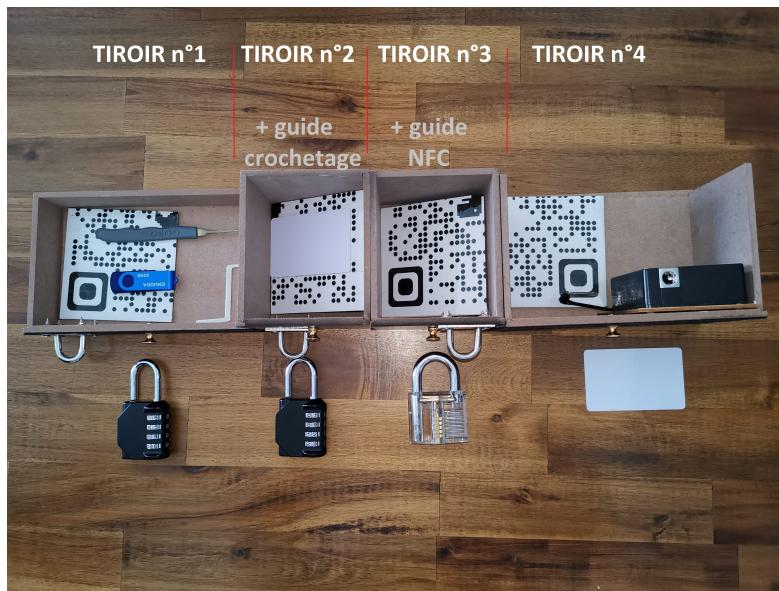
- Avez-vous trouvé un code dans la broyeuse ? (Off)
- Avez-vous trouvé le code de la clé usb bleue ? (Off)
- Avez-vous réussi à déverrouiller le cadenas à crocheter ? (Off)
- Avez-vous réussi à copier la carte NFC et déverrouiller le plus gros tiroir ? (Off)
- Avez-vous inséré la clé USB violette et activé les macros ? (Off)
- Avez-vous trouvé le fichier dans la corbeille du PC ? (Off)
- Etes-vous allé sur un site malveillant via l'une des deux faces du QR Code reconstitué ? (Off)
- Avez-vous trouvé le mot de passe d'Alexandre DUBOIS ? (Off)

Below this is a large text input field for general feedback, with the placeholder text 'Sentez-vous libre de donner votre avis sur l'escape game et de potentielles propositions quant à l'amélioration des challenges.' A blacked-out area follows, and at the bottom is a dark button labeled 'Envoyer mes réponses'.

Annexe 19 : Photo illustrant le meuble dans son intégralité et verrouillé



Annexe 20 : Photo illustrant le contenu des différents tiroirs



Annexe 21 : Document représentant la fiche de tests

ENTREPRISE		NB PARTICIPANTS	
Challenge	Temps	Difficulté	Notes
POST-IT			
BROYEUSE			
USB Mauvaise			
USB Bonne			
CORBEILLE PC			
CROCHETAGE			
NFC			
QR CODE			
CV/MDP			
SONDAGE			