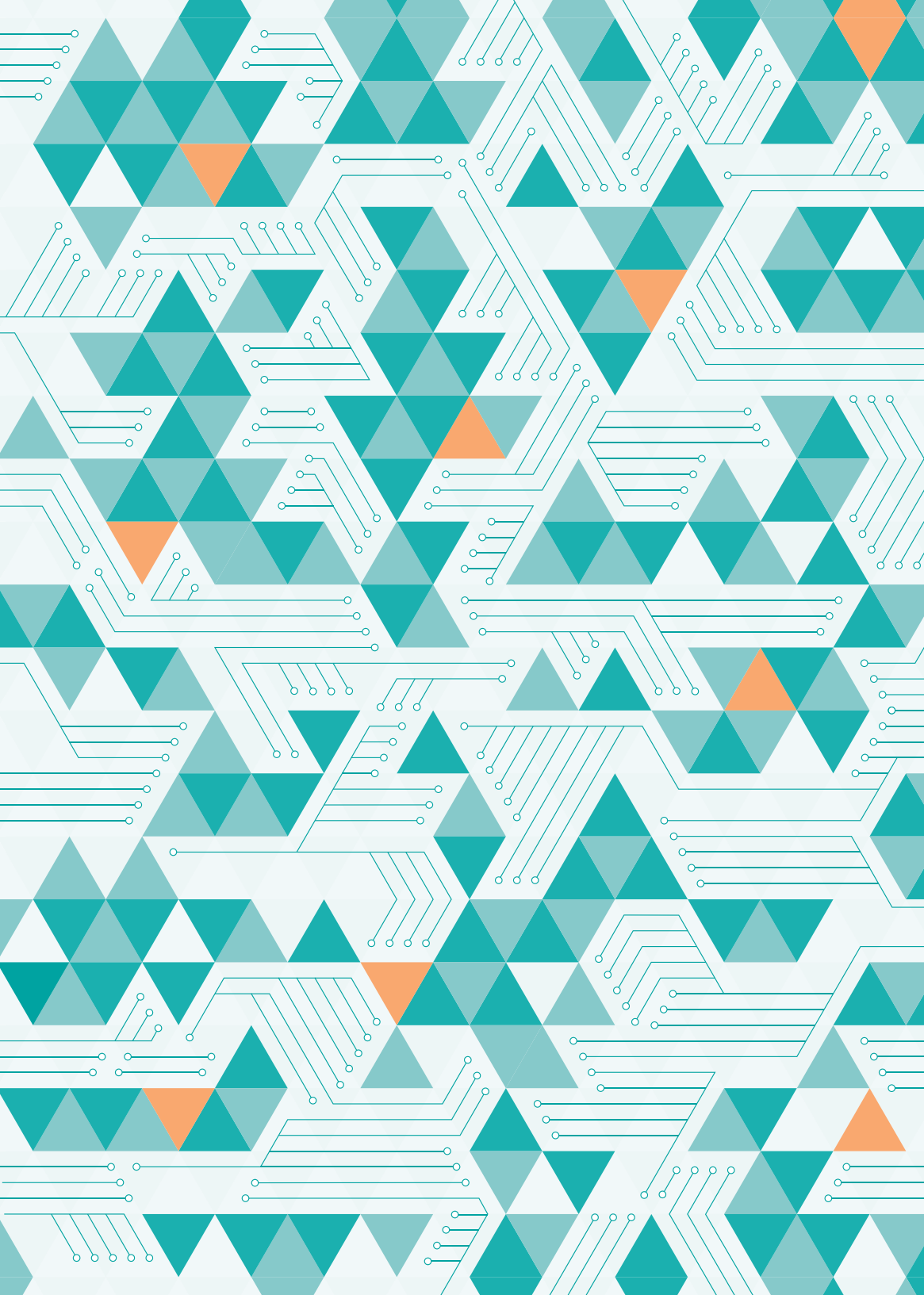
KryptoKids

Guide



Bienvenue dans le guide *KryptoKids*.

Si vous n'avez pas encore l'application, téléchargez-la depuis l'App Store.

Table des matières

Avant-propos **4**

Introduction **5**
Qu'est-ce que *KryptoKids* ? 5
Pourquoi la protection des données est-elle importante ? 6
Objectifs de *KryptoKids* 7
Recommandation par rapport à l'âge 8

Découvrir *KryptoKids* – contenu **9**
Intrigue 9
Protagonistes 9
- *KryptoKids* 9
- *Nina Niouse* 12
- *DataPieuvs* 12

Contenu 13
- Chapitre 1 – protection des données 13
- Chapitre 2 – sécurité des données 14
- Chapitre 3 – traces de données et piratage 15

Mettre en œuvre le projet *KryptoKids* – préparation **16**
Planification 16
Contenu de la mallette 18
Préparer le matériel et les moyens techniques 19
- Matériel – chapitre 1 21
- Matériel – chapitre 2 21
- Matériel – chapitre 3 21
- Matériel – clôture (facultatif) 21

Fonctionnement de la tablette 22
Codes 22

Mettre en œuvre le projet *KryptoKids* – déroulement 23
Préparer la pièce 23
Introduction 23
Jouer 23
- Chapitre 1 24
- Chapitre 2 24
- Chapitre 3 26

Clôture 26
Une fois *KryptoKids* terminé 27

Maîtriser *KryptoKids* – aide 28
Chapitre 1 28
- Menu 28
- *KryptoPuzzle* RA 29
- Jeu de collecte de données RA 29
- Estimer la valeur des données 29

Chapitre 2 30
- Sécurité du serveur 30
- Énigme de chiffrement, étape 1 : trouver le code 30
- Énigme de chiffrement, étape 2 : utiliser le code 31
- Sauvegarde de données RA 32

Chapitre 3 32
- Chasse aux virus 32
- Chasse aux virus RA 32

Jeux analogiques à faire entre-deux 33
- Carte *KryptoKids* 33
- Terrier 33
- Je protège mes données 34
- Chasse aux *DataPieuvs* 34

Problèmes éventuels et FAQ 35

Personnes et acteurs impliqués 36

Sources 36

Avant-propos

Chères lectrices et chers lecteurs,

Nous vivons dans un monde où de plus en plus de domaines de la vie sont influencés par la numérisation. Nous divulguons toutes et tous des données personnelles sur internet. La frontière entre nos actions conscientes et intentionnelles et nos actions inconscientes et involontaires n'est souvent pas très nette. Alors qu'advient-il de nos données ? Qui peut y accéder ? Comment sont-elles utilisées et sommes-nous au courant lorsque c'est le cas ? En bref : pourquoi la protection des données est-elle si importante ? L'application *KryptoKids* vous entraîne dans une histoire passionnante parsemée de nombreux mini-jeux. Elle répond d'une manière adaptée à l'âge des participant·e·s aux questions ci-dessus ainsi qu'à d'autres interrogations importantes concernant la protection et la sécurité des données. De cette manière, les enfants et les jeunes sont sensibilisés à ces sujets et développent leurs compétences numériques.

KryptoKids est un projet commun de la Fachstelle für Jugendmedienkultur NRW et de GLUON STUDIOS. Le projet a été soutenu par la Stiftung Deutsche Jugendmarke e.V. La Schauspielschule & Stageschool Salomon Academy a donné leur voix aux protagonistes de *KryptoKids*. En Suisse, c'est Jugendarbeit.digital qui est responsable de *KryptoKids*. Nous en profitons pour remercier ici toutes les personnes qui ont contribué à la création de *KryptoKids* !

Nous vous souhaitons bien du plaisir avec *KryptoKids* !

Introduction

Conditions générales qui prêtent à confusion et projets de loi peu compréhensibles : la protection des données n'est pas un sujet facile, c'est pourquoi les jeunes et les moins jeunes préfèrent souvent tout simplement l'ignorer. Le sujet semble trop abstrait et les risques possibles pas assez concrets. Dans un monde de plus en plus numérique, sensibiliser les enfants et les jeunes à cette problématique devient donc un véritable défi.

KryptoKids s'est donné pour mission d'amener les enfants et les jeunes dès leur plus jeune âge à aborder de manière ludique du thème de la protection de leurs données. Le jeu d'aventure sur tablette présente les thèmes du chiffrement, de la sphère privée et de la sécurité des données d'une manière adaptée au groupe cible.

Qu'est-ce que *KryptoKids* ?

L'élément central du projet est l'application *KryptoKids*, qui guide les enfants et les jeunes à travers un événement encadré pédagogiquement et rend ainsi les sujets tangibles en les abordant de manière ludique. Plongés dans une histoire captivante, les participant·e·s sont invité·e·s à élucider un vol sournois de données par l'exploration et la recherche. Ce faisant, les enfants développent à travers trois chapitres différents une compréhension de base de ce que sont la sphère privée, la sécurité des données et le chiffrement – également connu sous le nom de cryptographie.

L'application se charge de sensibiliser les participant·e·s à ces thèmes et de présenter le sujet complexe d'une manière appropriée au groupe cible. Les événements encadrés au niveau pédagogiques sont toutefois le cœur du projet. Les centres d'animation socioculturelle enfance et jeunesse, mais aussi les écoles et les bibliothèques, peuvent mettre en œuvre le projet *KryptoKids* de manière autonome. Outre les risques liés à la consommation de médias, le jeu aborde également les mécanismes et les effets du chiffrement. *KryptoKids* encourage les enfants et les jeunes à se percevoir comme des actrices et acteurs informés et critiques qui peuvent et doivent protéger leur vie privée.

L'application seule ne doit être comprise que comme un outil ; elle sert d'illustration ludique. Ce sont en effet l'encadrement et la présentation du contenu par les pédagogues qui sont l'élément central; les réflexions en groupe et les suggestions sont particulièrement importantes. Le guide a pour but de fournir des conseils sur les différentes possibilités d'aborder le sujet.

Tu peux mettre en œuvre le projet *KryptoKids* de manière autonome ou te renseigner à propos des alternatives que nous proposons en consultant notre site: www.krypto-kids.ch.

Pourquoi la protection des données est-elle importante ?

Lorsque nous naviguons sur internet, des données sont générées presque à chaque clic et à chaque saisie. Ces données peuvent être des recherches, des sites internet visités, des données personnelles et bien d'autres encore. Ces informations sont utilisées par des entreprises pour proposer des produits et des services de manière très ciblée. Cela signifie que si de nombreuses données sont collectées, les publicitaires peuvent en tirer profit sans que nous, utilisatrices et utilisateurs d'internet, ne soyons conscients de ce processus et n'y consentions d'une part, et d'autre part, sans que nous ne puissions en tirer profit.

Les données personnelles ont une place particulièrement importante dans la protection des données. Les données personnelles peuvent être le nom, l'adresse, l'âge, le courriel ou les numéros de téléphone, mais aussi les données de localisation ou l'accès aux applications. Ces données personnelles permettent de distinguer les utilisateurs et utilisatrices d'internet les un·e·s des autres et donc de les identifier en tant que personnes individuelles. En même temps, la technologie moderne des « appareils intelligents » comme les téléphones ou les tablettes que presque tout le monde possède augmente la possibilité d'être identifié·e, car de nombreuses applications que nous utilisons tous les jours ont accès au microphone, à l'appareil photo, aux carnets de contacts, etc. et rendent la collecte de données personnelles beaucoup plus opaque. Nous savons que ces données sont collectées, mais nous faisons souvent fi de notre méfiance saine à l'égard de la collecte de données la collecte de données, parce que nous voulons utiliser les services pratiques et amusants des applications et des fournisseurs de plateformes sans trop de restrictions. Mais souvent aussi, nous agissons ainsi malgré notre méfiance parce qu'il est incroyablement difficile de savoir qui accède, stocke et analyse quelles données et ce qu'il se passe avec cette analyse.

Mais l'esprit critique est important pour pouvoir le plus possible déterminer soi-même ce qu'il se passe avec ses informations. La protection contre l'utilisation abusive des données personnelles est ancrée dans la Constitution fédérale (art. 13). Pour cette protection, une plus grande transparence et davantage de connaissances concernant ce que l'on peut appeler les « pieuvres informatiques » sont nécessaires. Car le vol de données et l'utilisation abusive de données personnelles peuvent avoir de graves conséquences pour chacun·e d'entre nous.

Objectifs de *KryptoKids*

KryptoKids a pour but de faire des enfants des utilisatrices et utilisateurs de médias compétents. La matière est transmise en trois chapitres. Le premier chapitre porte sur ce que sont les données personnelles. Les utilisatrices et utilisateurs sont amenés à prendre conscience de la valeur de ces données et à reconnaître qu'elles doivent être protégées. Le chapitre 2 est consacré à la sécurité des données. L'application montre comment le chiffrement, les mises à jour de sécurité, les pare-feux et les programmes antivirus peuvent être utilisés pour renforcer la sécurité de nos données. Le troisième chapitre traite des traces que nous laissons sur internet, de ce que sont les adresses IP, de la manière de se protéger des attaques de pirates informatiques et de la manière de se comporter si nous sommes victimes d'un vol de données.

Les objectifs d'apprentissage sont axés principalement sur l'acquisition de compétences médiatiques. Le projet est basé sur la définition de la compétence médiatique de Dieter Baacke. Ce dernier considère l'être humain comme un sujet qui agit de manière active. Selon cette définition, l'individu peut participer de manière active à cofaçonner son environnement et porte une responsabilité propre.

Les différents chapitres de *KryptoKids* reprennent en particulier les deux premières dimensions du modèle de compétence médiatique de Baacke (critique des médias et étude des médias). Grâce au fait qu'elle encourage la réflexion critique par rapport aux contenus proposés, l'application *KryptoKids* développe les connaissances des enfants d'une manière adaptée à leur âge. Ces connaissances de base permettent aux enfants d'examiner et d'élargir leurs propres actions en matière de protection et de sécurité des données. L'approche ludique permet la prise de conscience (souvent difficile) de l'intérêt que des étrangers peuvent avoir pour les données personnelles d'autres individus. À travers de nombreuses interactions, *KryptoKids* promeut la proactivité, c'est-à-dire la conscience de la manière dont on peut influencer l'évolution des événements de manière autodéterminée et par une action prospective. Dans *KryptoKids*, chaque individu devient une personne active.

Dans une optique d'éducation aux médias, *KryptoKids* explique des termes importants tels que pirate informatique, hameçonnage, virus et pare-feu, qui sont ensuite appris et intégrés grâce à une approche ludique.

Dans le domaine de l'éducation, les jeunes ne sont généralement familiarisés avec les défis de la protection des données et de la vie privée qu'au cycle 2. On peut trouver une variété de méthodes, de programmes et de matériel pédagogique à cette fin. Cependant, les enfants ont souvent accès plus tôt à leurs propres appareils, tels que des smartphones, et

surfent sur internet ou utilisent des applications sans les remttre en question de manière critique. Il est donc nécessaire de s'occuper de la protection des données dès le cycle 1. Nous voulons que les enfants sachent ce qu'est un mot de passe sécurisé avant même de recevoir leur premier mot de passe. *KryptoKids* est un programme de prévention important et nécessaire, qui sensibilise tôt à ce thème.

Tu trouves de plus amples informations sur le thème de la protection des données sur notre site web www.krypto-kids.ch.

Recommandation par rapport à l'âge

L'âge recommandé pour *KryptoKids* est basé sur l'évaluation pédagogique d'éducatrices et d'éducateurs aux médias très expérimentés qui ont été largement impliqués dans le développement de l'application. Pour les enfants de moins de 8 ans, les sujets relatifs à la protection des données sont généralement difficiles à comprendre en raison de leur méta-niveau et de leur complexité. En outre, un niveau de base en lecture et en compétences médiatiques est requis, surtout pour l'utilisation de la tablette. Pour les enfants de 14 ans et plus, en revanche, la présentation et les mécanismes du jeu pourraient rapidement sembler trop ennuyeux et décevants. Tout dépend toutefois des expériences faites précédemment avec les médias et du stade de développement des jeunes. Lors de la conception de l'application, nous avons défini comme groupe cible central la tranche d'âge des 8 à 12 ans.

Découvrir *KryptoKids* – contenu

Intrigue

Les *KryptoKids* reçoivent sur leur tablette une nouvelle de dernière minute : la nuit dernière, une attaque de pirates informatiques a eu lieu dans toute l'Europe ! Le groupe criminel des *DataPieuvs* serait à l'origine du vol. Les pirates ont volé toutes les adresses privées, mots de passe, données de chats et données bancaires des citoyen·ne·s. Heureusement, la police a fait des *KryptoKids* son unité spéciale. Car Filippa, Samira, Ben et Flo sont de vrais geeks et des pros du piratage, de la programmation et du chiffrement. Pourront-ils sauver les données avant que les méchant·e·s ne puissent en profiter ?

Protagonistes

KryptoKids

Les quatre ami·e·s se retrouvent régulièrement dans leur base secrète, la centrale des *KryptoKids*. Le lieu est inconnu. Outre leur passion commune pour la protection des données et les innovations techniques, ils ont chacun des particularités et des loisirs différents.

Flo

Nom	Flo
Âge	14 ans
Spécialité	Piratage
Loisirs	Natation, jeux vidéo

Premières expériences techniques

Flo est un joueur passionné. Après une dispute, sa mère a verrouillé avec un mot de passe son ordinateur avec tous ses jeux. Flo a ensuite découvert sur internet qu'on peut craquer certains mots de passe assez facilement. Il a en fait réussi à pirater son propre ordinateur, ce qui l'a totalement surpris et fasciné. Après cela, il est retourné auprès de sa mère et l'a aidée à définir des mots de passe sûrs pour tous les appareils de la maison. Plus tard, il a également contribué dans son école et même auprès de la police à découvrir des failles de sécurité et est ainsi devenu, grâce au piratage, un expert recherché en sécurité.

Benny

Nom	Benny
Âge	11 ans
Spécialité	Recherche
Loisirs	Football, photographie

Premières expériences techniques

Dans le cadre d'un concours organisé à l'école, Ben a gagné comme prix un ordinateur avec un système d'exploitation open source, et l'a formaté tout seul à l'aide du manuel fourni avec l'ordinateur. Étant donné qu'un programme de photographie qu'il aurait voulu installer n'était pas disponible pour son système d'exploitation, il a réécrit le programme à l'aide de vidéos YouTube pour qu'il fonctionne sur son ordinateur.

Filippa
(sœur jumelle de Samira)

Nom	Filippa
Surnom	Flippa
Âge	13 ans
Spécialité	Programmation
Loisirs	Synthétiseur et chant

Premières expériences techniques

Filippa est une musicienne passionnée dans un groupe de musique. Par le fait qu'elle joue du piano, elle a découvert il y a quelques années ce qu'est un synthétiseur et a appris à l'utiliser. C'est ainsi qu'elle a fait ses premiers pas dans la programmation. Elle aime combiner la musique et la technologie.

Samira
(sœur jumelle de Filippa)

Nom	Samira
Surnom	Sam
Âge	13 ans
Spécialité	Chiffrement
Loisirs	Chevaux

Premières expériences techniques

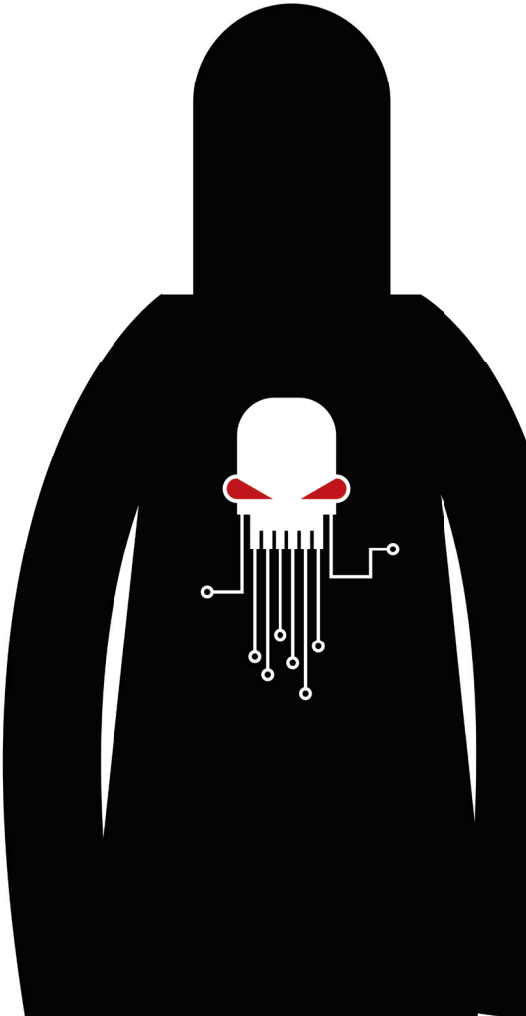
Samira aime les maths plus que tout. Elle consacre également beaucoup de temps à ce sujet pendant son temps libre. Lorsque sa sœur Filippa a eu besoin d'aide avec son synthétiseur parce qu'elle était bloquée par certaines formules, elle l'a aidée avec ses connaissances mathématiques et a ainsi découvert un nouveau domaine d'intérêt.

Nina Niouse

Nina Niouse est la porte-parole de News TV. Dans sa fonction, elle présente les nouvelles et explique les faits. Elle apparaît dans le chapitre 1 et dans le chapitre 3.

DataPieuvs

Les *DataPieuvs* sont une organisation criminelle fictive qui collecte des informations numériques dans le monde entier à des fins lucratives. Les *DataPieuvs* piratent des systèmes informatiques, volent des données et les vendent aux plus offrants sur le marché noir.



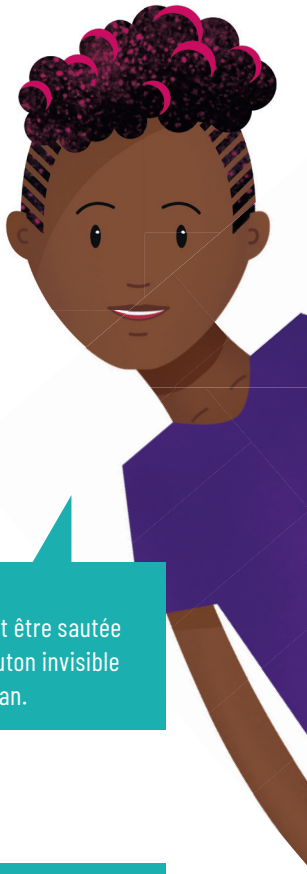
Contenu

Chapitre 1 – protection des données

#DonnéesPersonnelles #MotsDePasseSûrs
#CompétencesMédiatiques #Applications

Au début, les joueuses et joueurs sont invités à indiquer leur prénom, leur nom, leur âge et leur sexe. Le chapitre 1 commence ensuite par une séquence filmée d'environ trois minutes. Les *KryptoKids* regardent le journal télévisé. La présentatrice *Nina Niouse* annonce un important vol de données. À la fin de la séquence vidéo, l'organisation responsable du vol de données détourne la transmission du journal télévisé. Les *DataPieuvs* exposent clairement leurs motivations : ils veulent vendre les données personnelles volées aux plus offrants. Les CrytoKids veulent empêcher cela avec l'aide des participant·e·s et des *KryptoPads* (tablettes).

Après avoir regardé la vidéo, les enfants peuvent jouer à *KryptoKids*. Un court tutoriel présente les applications internes au jeu. Les joueurs et joueuses reçoivent un courriel de Filippa leur demandant de localiser et de scanner les dossiers de données (classeurs). Cette étape est suivie de la première énigme et du mini-jeu réalité augmentée (voir les explications du jeu pour plus de détails). Après avoir scanné chaque marqueur, ils doivent donner une estimation de la valeur des données qu'ils ont trouvées. Une fois que les quatre marqueurs ont été scannés et que les données ont été estimées, le deuxième chapitre commence.



Remarque :
La séquence vidéo peut être sautée en appuyant sur un bouton invisible en bas à droite de l'écran.

Remarque :
Dans la section « Aide » du manuel, tu trouves une explication de ce que signifie RA ainsi que des consignes de jeu.

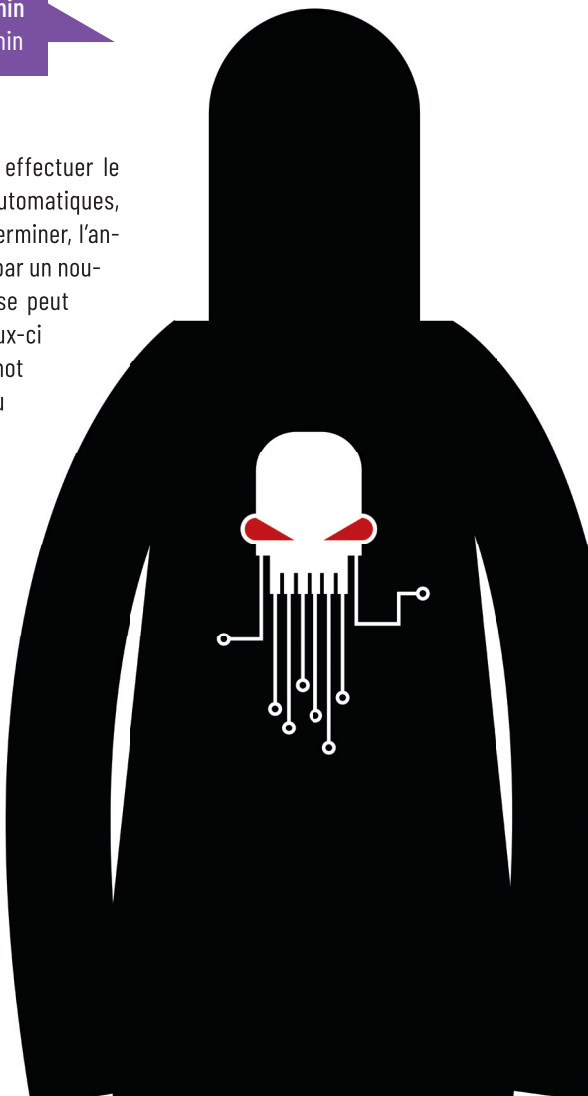
Chapitre 2 – sécurité des données

#Chiffrement #SécuritéDuServeur #PareFeu #MisesÀJour #Antivirus #AnalyseAntivirus

Le chapitre 2 commence par une séquence vidéo d'environ une minute. Les *KryptoKids* remercient les participant·e·s pour leur aide. Grâce à eux, les données piratées ont été retrouvées. Pour éviter que les données ne soient à nouveau volées, elles doivent être cryptées et les serveurs doivent être protégés. Pour cela, les *KryptoKids* envoient par courriel aux joueurs et joueuses les données d'accès de l'application de sécurité du serveur nouvellement installée :

Nom d'utilisateur ou d'utilisatrice : **admin**
Mot de passe : admin

Les joueurs et joueuses doivent maintenant effectuer le test du système en activant les mises à jour automatiques, le pare-feu et le programme antivirus. Pour terminer, l'ancien mot de passe (admin) doit être remplacé par un nouveau mot de passe sécurisé. Le mot de passe peut être choisi par les participant·e·s, mais ceux-ci doivent respecter les règles concernant le mot de passe qui sont indiquées à côté. Le nouveau mot de passe doit ensuite être crypté à l'aide du cadran de César. Le serveur est maintenant protégé grâce aux mises à jour et au mot de passe sécurisé. Ensuite, les participant·e·s reçoivent un courriel des *KryptoKids* auquel est joint un courriel crypté des *DataPieuvs* qui a été intercepté. Ce message doit être décodé en utilisant le cadran de César. La solution du premier message donne un indice sur la clé utilisée pour chiffrer le message suivant. Décrypté, cela signifie : DEVONS PIRATER LES *KRYPTOKIDS* AVANT QU'ILS NE NOUS TROUVENT !



Pour parer à l'attaque des *DataPieuvs*, les données exemptes de virus doivent être replacées dans les classeurs et cryptées. Pour ce faire, il faut utiliser le *KryptoScanner* pour scanner à nouveau les classeurs et insérer les données dans les classeurs à l'aide d'un mini-jeu RA.

Chapitre 3 – traces de données et piratage

#TracesSurLeNet #Piratage #CourrielDHameçonnage #Localisation

Une fois les virus éliminés et les données sécurisées, les *DataPieuvs* lancent une nouvelle attaque contre la centrale des *KryptoKids*. Les joueurs et joueuses reçoivent un courriel qui semble avoir été envoyé par Filippa, mais qui est en fait un courriel d'hameçonnage. Après avoir ouvert la pièce jointe, le *KryptoPad* est infesté de virus. Ceux-ci doivent être éliminés dans un mini-jeu de type « pointer-cliquer » ainsi que dans un autre jeu de RA. Une fois l'ennemi final (supervirus) combattu, les joueurs et joueuses obtiennent l'adresse IP des *DataPieuvs*, qui fournit des informations sur leur localisation géographique. Après avoir trouvé l'adresse exacte, les participant·e·s peuvent contacter la police. Objectif atteint ! Les *DataPieuvs* ont été trouvés et arrêtés grâce à l'aide des joueurs et joueuses.

Mettre en œuvre le projet *KryptoKids* – préparation

Planification

- Lire le guide et se renseigner sur le sujet et le jeu (tu es en train de le faire, super).
- Organiser le matériel et les moyens techniques, désigner les personnes chargées de la mise en œuvre du projet.
  - Consulter www.krypto-kids.ch. Il existe maintenant trois options :

1. Pour réaliser le jeu, tu utilises ton propre équipement technique, tu télécharges le matériel sur la page d'accueil et l'imprimes. Ensuite, tu dois découper certains des documents imprimés et les assembler (en option, les participant·e·s peuvent t'aider à le faire).

2. Tu commandes (en prêt) la mallette *KryptoKids* qui contient l'équipement technique et le matériel nécessaire, et tu mets en œuvre le projet *KryptoKids* de manière autonome.

3. Via notre site internet, tu fais appel aux services d'un·e spécialiste en pédagogie des médias qui réalise le projet *KryptoKids* dans votre établissement et apporte la mallette ainsi que tout le matériel.

Conseil :
Nous te recommandons de jouer au préalable une fois toi-même à *KryptoKids* du début à la fin et de nous contacter si tu as des questions ou des suggestions.

- Organiser des participant·e·s/faire de la publicité
  - Tu peux commander du matériel publicitaire sur www.krypto-kids.ch (comprend des prospectus, des affiches, des autocollants et des autocollants pour masquer la caméra d'ordinateurs portables/tablettes et de téléphones, avec design *KryptoKids*).

- Organiser un local pour la mise en œuvre du projet
  - Pour les groupes de six personnes ou plus, la pièce doit offrir la possibilité de s'isoler un peu, sinon l'endroit sera trop bruyant pour une utilisation pertinente de l'application. Pour un groupe de dix personnes ou plus, nous recommandons d'utiliser deux pièces.

- Fixer une ou des dates
  - Il n'est pas nécessaire de finir tous les chapitres en une seule fois. Tu peux également les répartir sur plusieurs jours. Vous aurez ainsi plus de temps pour discuter du contenu et approfondir la réflexion.

Contenu de la mallette

4 classeurs vides avec des marqueurs RA

Boîte avec
- 4 câbles d'alimentation
- Station de charge
- Imprimante photo

4 iPads dans des étuis de protection, avec l'application *KryptoKids* déjà installée

Boîte avec
- Cartes de quiz et carte à filtre rouge
- Badges
- Cadrans de César

Guide

Guide de démarrage rapide

Préparer le matériel et les moyens techniques

- Commander la mallette (en prêt), suivre le Guide de démarrage rapide (charger les tablettes avant le jeu, les allumer, lancer l'application, activer le mode « accès guidé »).

OU

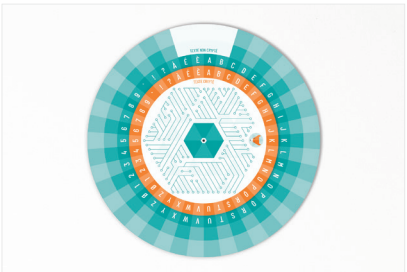
- Installer *KryptoKids* sur vos propres tablettes.
- Imprimer et préparer les documents à imprimer (ou bien bricoler avec les participant·e·s).
- Pour réaliser le cadran de César, vous aurez besoin d'attaches parisiennes, de ciseaux et d'un objet pointu pour percer un trou (comme un poinçon). Veiller à placer l'attache parisienne exactement au centre.
- Carte à filtre rouge pour quiz (en option) :
  - Comme son nom l'indique, le filtre rouge filtre la couleur rouge (en l'occurrence le charabia rouge qui recouvre la réponse au dos de la carte) et ne laisse passer que la couleur noire (la réponse). Cela permet de lire la réponse sur la carte de quiz. Il existe également une version quiz à télécharger qui peut être utilisée sans carte à filtre rouge. Tu trouves davantage d'informations sur le quiz dans le chapitre Mettre en œuvre le projet *KryptoKids* – déroulement.

Classeurs avec *KryptoMarqueur*

Badges *KryptoKids*

Tablettes avec *KryptoKids*

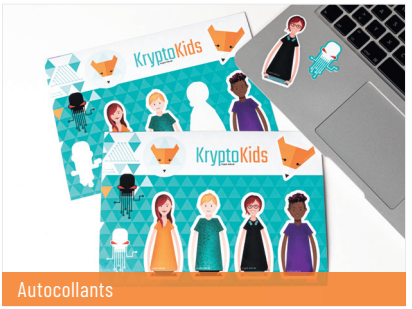
Cartes de quiz avec carte à filtre rouge



Cadran de César

Imprimante photo

Autocollants pour masquer la caméra d'un téléphone portable ou autre



Autocollants

Matériel – chapitre 1

- 4 classeurs avec *KryptoMarqueur* (orange, bleu, lila, noir)
- Badges/cartes *KryptoKids* (1 pour chaque participant·e)
- Tablettes avec *KryptoKids* (1 pour 1 à 3 participant·e·s)
- Cartes de quiz avec questions 1 à 3
- Carte à filtre rouge (facultatif)

Conseils :

- Pour les groupes de grande taille, il est recommandé de distribuer plusieurs séries de *KryptoMarqueurs*.
- Au lieu d'un badge, les participant·e·s peuvent également recevoir une carte ou un autocollant. Les badges peuvent aussi être bricolés en groupe !
- Nous recommandons que 1 à 3 participant·e·s partagent une tablette et jouent ensemble à *KryptoKids*.

Matériel – chapitre 2

- Cadran de César
- 4 classeurs avec *KryptoMarqueur* (orange, bleu, lila, noir)
- Cartes de quiz avec questions 4 à 5
- Carte à filtre rouge (facultatif)

Matériel – chapitre 3

- Cartes de quiz avec questions 6 à 7
- Carte à filtre rouge (facultatif)

Matériel – clôture (facultatif)

- Certificat
- Autocollants
- Autocollants pour masquer la caméra d'un téléphone portable ou autre
- Imprimante photo

Fonctionnement de la tablette

Codes

CODES

Dans le jeu :

Remettre le jeu au début :	4242
Déverrouiller le chapitre 2 :	0002
Déverrouiller le chapitre 3 :	0003

Tablette :

Déverrouiller :	50825
Mode « accès guidé » :	112020

Mallette :

Cadenas :	404

Mettre en œuvre le projet *KryptoKids* – déroulement

Préparer la pièce

- Cacher les classeurs/*KryptoMarqueurs* à différents endroits
- Disposer le matériel

Introduction

- Trouver un jeu pour l'accueil/pour faire connaissance (conseils dans la section « Aide » du guide).
- Expliquer *KryptoKids*. Qu'est-ce que *KryptoKids* ? Qu'allons-nous faire aujourd'hui ?
- Discuter des règles relatives à l'utilisation de l'équipement technique.
- Expliquer aux participant·e·s qu'après chaque chapitre vous allez vous réunir pour une séance de réflexion en groupe et que le ou la responsable du jeu leur donnera ensuite le mot de passe dont ils auront besoin pour commencer le chapitre suivant.
- En outre, il est utile qu'après chaque chapitre les participant·e·s racontent avec leurs propres mots ce qu'il s'est passé et ce qu'il a fallu faire.

Sujets de réfléxion :

- Avez-vous accès à internet ? Si oui, comment (smartphone, ordinateur portable, tablette, smartphone des parents) ?
- Avez-vous déjà indiqué votre nom quelque part sur internet ?
- Est-ce que vous vous sentez en sécurité sur internet ?

Jouer

- L'application va maintenant vous guider dans le jeu. Si tu rencontres des problèmes avec les mécanismes du jeu ou le matériel, lis les conseils dans la section « Aide » du guide.
- Tous les termes techniques sont expliqués dans le wiki du jeu. Le wiki est élargi au fur et à mesure que chaque chapitre est complété. Ainsi, il n'est complet qu'au début du dernier chapitre.

Chapitre 1

Pour commencer le premier chapitre, les questions 1 à 3 du quiz sont passées en revue avec les participant·e·s afin de clarifier les concepts importants du chapitre.

Sujets de réflexion :

- Pourquoi la protection des données est-elle importante ?
- Où divulguez-vous vos données personnelles ?
- Utilisez-vous les médias sociaux ?
- Avez-vous déjà été piraté·e·s ?
- Pourquoi des personnes que vous ne connaissez pas sont-elles intéressées par vos données ?

Saisie de données avant le début du jeu :

La saisie de données doit faire l'objet d'une réflexion ! Ici, les participant·e·s saisissent leurs données sans raison. Ils doivent être sensibilisés à ne pas indiquer leurs données personnelles sur internet uniquement parce qu'on leur demande de le faire.

Sujets de réflexion :

- Est-il possible de faire tout cela avec un faux nom ou sans nom du tout ?
- Qu'est-ce qui pourrait se passer si je communique mon vrai nom sur internet ?

Badge *KryptoKids* après la séquence vidéo :

Après la séquence, chaque participant·e au jeu reçoit un badge ou une carte *KryptoKids*. Cela permet une plus grande identification au groupe et augmente le sentiment d'agir comme un soutien pour les *KryptoKids*.

Tâche d'estimation de la valeur des données :

Les différentes données ont plus ou moins de valeur. La tâche d'estimation doit faire l'objet d'une réflexion avec les participant·e·s.

Sujets de réflexion :

- Quelles sont les données particulièrement précieuses ? Pourquoi ?
- Ces données sont-elles seulement vendues illégalement sur le marché noir ? Ou vos données peuvent-elles aussi être transmises tout à fait légalement ?

Chapitre 2

En introduction au deuxième chapitre, les questions 4 et 5 du quiz sont discutées avec les participant·e·s afin de clarifier les termes importants du chapitre.

Sécurité du serveur :

Après avoir reçu le courriel contenant les informations d'identification (nom d'utilisateur ou d'utilisatrice admin, mot de passe admin) et après avoir sécurisé le serveur, discutes avec les participant·e·s des règles en lien avec la gestion des mots de passe.

Sujets de réflexion :

- Qu'est-ce qui ne doit en aucun cas être un mot de passe ?
- Qu'est-ce qui caractérise les mauvais mots de passe ?
- Qu'est-ce qui caractérise les bons mots de passe ?
- À qui dois-je confier mon mot de passe ?
- Quel est le but d'un pare-feu, d'une mise à jour et d'un programme antivirus ?

Chiffrement :

Il convient maintenant d'expliquer en détail le cadran de César. L'expérience a montré que l'animation explicative dans la vidéo n'est pas suffisante. Une explication détaillée est donnée dans la section « Aide » de ce guide. À l'aide du cadran de César, son propre mot de passe peut être crypté comme on le souhaite : il suffit de tourner le disque comme on le désire.

Sujets de réflexion :

- Pour quoi utilise-t-on un cadran de César ?
- Pourquoi le chiffrement est-il important ?

S'ensuit la partie la plus difficile du jeu. Ici, tu dois aider les participant·e·s à créer une atmosphère calme, car ils auront besoin de concentration pour terminer avec succès la partie qui suit.

La frustration peut rapidement apparaître lorsque les participant·e·s sont confronté·e·s au défi du processus de chiffrement et de déchiffrement. Il est donc utile de leur offrir une certaine aide. Tu trouves des instructions et la solution dans la section « Aide » de ce guide.

Sujets de réflexion :

- Qu'avons-nous fait dans le jeu RA pour sauvegarder les données ? (Nous avons remis les données dans les dossiers (classeurs). Ceux-ci sont désormais protégés par un mot de passe).
- Sommes-nous désormais à l'abri d'un vol de données ? Que pourraient faire les pirates pour accéder à ces données ?

Chapitre 3

En introduction au troisième chapitre, les questions 6 et 7 du quiz sont discutées avec les participant·e·s afin de clarifier les concepts importants du chapitre.

Courriel d'hameçonnage :

Après la vidéo d'introduction, les *KryptoKids* reçoivent un courriel d'hameçonnage. Les participant·e·s sont invité·e·s à ouvrir une pièce jointe d'un courriel.

Sujets de réflexion :

- Que disait le courriel de « Filppa » ? Qu'était-il écrit dans le courriel de « Filppa » ?
- Avez-vous tout de suite ouvert la pièce jointe ? Ou est-ce que quelque chose vous a semblé étrange ?
- Comment pouvons-nous reconnaître les courriels d'hameçonnage ? (Fautes d'orthographe, vérifier l'expéditeur, invitation à cliquer sur des liens/ouvrir des pièces jointes).
- Que sont les virus ? Et que font-ils à vos appareils ?
- À quoi remarquez-vous que votre appareil est infecté par des virus ? Que pouvez-vous faire pour les éliminer ? (Scanner de virus, l'appareil devient anormalement chaud et lent, des erreurs apparaissent continuellement, parlez-en à un adulte et demandez de l'aide).

Adresse IP :

Il ne te reste plus qu'un jeu RA avant de trouver les *DataPieuvs*. Après avoir vaincu le supervirus (ennemi final), tu obtiens l'adresse IP des *DataPieuvs* et donc leur localisation.

Sujets de réflexion :

- Qu'est-ce qu'une adresse IP ? (L'adresse IP d'un ordinateur est comme l'empreinte digitale d'une personne. Il s'agit en fait d'une séquence spécifique de chiffres qui ne peut être attribuée qu'à un seul ordinateur. Avec ton adresse IP, tu laisses des traces sur internet qui permettent de remonter jusqu'à ton appareil. Si l'appareil est sur internet, l'adresse IP peut être utilisée pour déterminer l'emplacement de l'appareil).

Clôture

La clôture du projet, en particulier, doit être encadrée de manière pédagogique. Après avoir traversé avec succès les trois chapitres, les participant·e·s peuvent prendre un selfie avec les *KryptoKids*. Pour accéder aux photos, il faut mettre quitter le mode « accès guidé » de la tablette et ouvrir la galerie photos. Les photos peuvent être imprimées avec une impri-

mante photo et doivent finalement être supprimées de la tablette avec les enfants. Les participant·e·s reçoivent un certificat en récompense de leur excellente performance. En option, vous pouvez commander via notre site internet des autocollants au design de *KryptoKids* et des autocollants pour masquer la caméra, que vous pouvez également offrir aux participant·e·s en guise de cadeau. Les badges/cartes *KryptoKids* peuvent être conservés par les enfants et les jeunes.

Sujets de réflexion :

- Pourquoi la protection des données est-elle importante ?
- Qu'avez-vous appris ?
- Qu'est-ce qui vous a plu ?
- Qu'est-ce qui vous a moins plu ?
- Que recommanderiez-vous à d'autres enfants et jeunes pour mieux se protéger sur internet ?

Une fois *KryptoKids* terminé

Uniquement dans le cas du prêt de mallette : faire l'inventaire/vérifier l'état des appareils, ranger le matériel, renvoyer la mallette. Les prospectus, les badges et les autocollants permettant de masquer la caméra d'un portable ou autre peuvent être conservés.

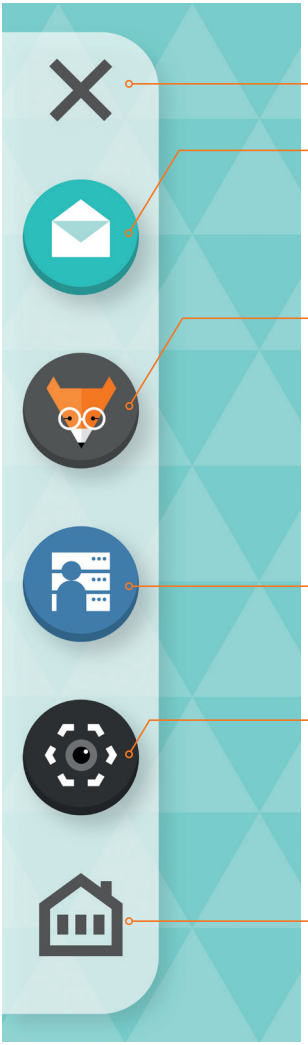
Par ailleurs : nous serions ravi·e·s que tu nous contactes après l'événement pour nous dire comment s'est déroulé le projet, où tu as organisé *KryptoKids* et avec combien de participant·e·s ! Cela nous aidera à améliorer et à développer *KryptoKids*. Le mieux est de nous écrire un courriel à info@krypto-kids.ch.

Note :
Tous les selfies ont-ils été effacés de l'iPad ?

Maîtriser *KryptoKids* – aide

Chapitre 1

Menu



Fermer le menu

Courriel

Les messages destinés aux joueurs et joueuses peuvent être ouverts via l'application de messagerie.

Wiki

De nombreux termes techniques sont utilisés dans *KryptoKids*. Vous pouvez consulter leurs définitions dans le wiki. De nouvelles entrées sont ajoutées à chaque chapitre. Ainsi, au début, seuls les termes du chapitre 1 sont accessibles.

Données

Les ensembles de données scannés sont traités et analysés dans la base de données.

KryptoScanner

Le *KryptoScanner* utilise la fonction caméra de la tablette. Il peut être utilisé pour scanner les *KryptoMarqueurs* (sur les classeurs). Il permet également d'activer les mini-jeux RA.

Retour à la vue d'ensemble des chapitres

KryptoPuzzle RA

Le *KryptoScanner* est utilisé pour scanner les *KryptoMarqueurs*. Ceux-ci ne doivent pas être placés directement les uns à côté des autres ! Pour la numérisation, une distance d'environ 80 cm est nécessaire. Un cube apparaît. Ce cube doit être tourné à l'aide des flèches afin qu'il ressemble exactement au *KryptoMarqueur* sur le classeur.

Remarque :
RA signifie « réalité augmentée ». Cela signifie que des éléments numériques sont ajoutés à la réalité (capturée par la caméra de la tablette) à l'aide d'une technologie moderne.

Jeu de collecte de données RA

Ce jeu commence juste après le *KryptoPuzzle* RA. Dans ce jeu, il s'agit d'attraper les données volantes (représentées par des petits triangles) avec le *KryptoPad*. Tu dois veiller à trouver la bonne distance. Celle-ci est d'environ 80 cm, mais peut être réduite si nécessaire. Lorsque les données sont collectées, cela est signalé par un son. Une fois que toutes les données ont été collectées, le jeu continue.

Conseil :
Les *KryptoMarqueurs* doivent continuer à être visés par la caméra pendant le jeu.

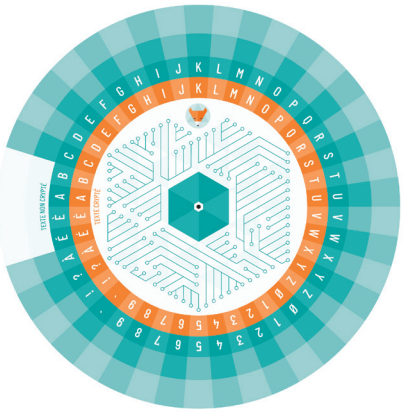
Estimer la valeur des données

Après chaque classeur scanné, les données collectées apparaissent dans la base de données. Vous y trouverez également une description du type de données (par exemple, données de base, données de communication, données de navigation, données bancaires). Ici, vous devez estimer ce que valent les différentes données sur le marché noir. Pour cela, déplacez le curseur. Cliquez ensuite sur « Solution ».

Chapitre 2

Sécurité du serveur

Il faut cliquer sur divers curseurs et icônes pour augmenter la sécurité de la tablette. Ainsi, les mises à jour sont installées, le pare-feu et un antivirus sont activés et un mot de passe sécurisé est choisi. Pour ce dernier, vous aurez besoin du cadran de César.



Le cadran de César est utilisé pour crypter les différentes lettres. Il peut être utilisé pour crypter des mots isolés tels que des mots de passe, mais aussi des phrases complètes et des messages. Il sert à illustrer les principes de base de la cryptographie. Chaque lettre du cadran de César est associée à une lettre cryptée. Les lettres sont présentées sur un disque extérieur (lettres non cryptées) et un disque intérieur plus petit (lettres cryptées). Le disque le plus petit peut être déplacé à volonté, de sorte que le chiffrement puisse être modifié en permanence.

Énigme de chiffrement, étape 1 : trouver le code

Maintenant, un message des *DataPieuvs* doit être décrypté. La première étape consiste à trouver le code. Pour cela, vous utilisez également le cadran de César. Cette énigme est complexe. Vous passez en revue chaque lettre l'une après l'autre. Vous voyez dans la zone supérieure que le chiffre 4 du texte non crypté correspond en forme crypté au chiffre 7. Tournez le cadran de César de telle sorte que 4 et 7 soient l'un en dessous de l'autre. Regardez

ensuite sur le cadran de César sous quelle lettre, quel caractère ou quel chiffre se trouve la lettre « I ». Vous devriez maintenant la trouver sous F.

Passe maintenant à la lettre suivante. Tourne le cadran de César de telle sorte que le M se retrouve sous le A. Cela signifie qu'au-dessus du 6 tu trouves le U.

Fais de même avec les autres positions cryptées. Tourne le cadran de César comme décrit ci-dessus, décrypte le texte crypté, tourne à nouveau le cadran, décrypte, etc.

La solution correcte est :
RENARD SUR D

Énigme de chiffrement, étape 2 : utiliser le code

Sur le cadran de César, tu vois le symbole du renard. Tourne le cadran de César de telle sorte que le renard soit dirigé vers la lettre D (RENARD SUR D). Utilise maintenant le code pour décrypter le message. Cette fois, tu n'as pas à tourner encore le cadran de César. Il te suffit de lire les lettres du disque extérieur. Si tu saisis une lettre, un chiffre ou un caractère erroné, il sera marqué en rouge.

La solution correcte est :
DEVONS PIRATER LES *KRYPTOKIDS* AVANT QU'ILS NE NOUS TROUVENT !

Sauvegarde de données RA

Dans ce mini-jeu, tu dois catapulter les données dans les classeurs et les sauvegarder. Pour ce faire, clique dans le champ de saisie en bas à gauche. Tu définis la direction en déplaçant la tablette. Vise le triangle rouge. Nous recommandons une distance d'environ 50 cm. Lorsque tu as bien visé, le cube s'emballe et un marquage carré apparaît. Tu dois maintenant tenir la tablette de telle sorte que le cube soit à l'intérieur du marquage. Nous recommandons une distance d'environ 30 cm. Maintenant, tu dois cliquer sur « Crypter » en bas à droite. Dans une animation, les données dans le cube sont cryptées. Répète ce procédé pour chaque *KryptoMarqueur*.

Conseil :
Les *KryptoMarqueurs* doivent continuer à être visés avec la caméra pendant le jeu. Si un *KryptoMarqueur* ne fonctionne pas correctement, il est souvent utile d'essayer d'abord avec un autre *KryptoMarqueur*.

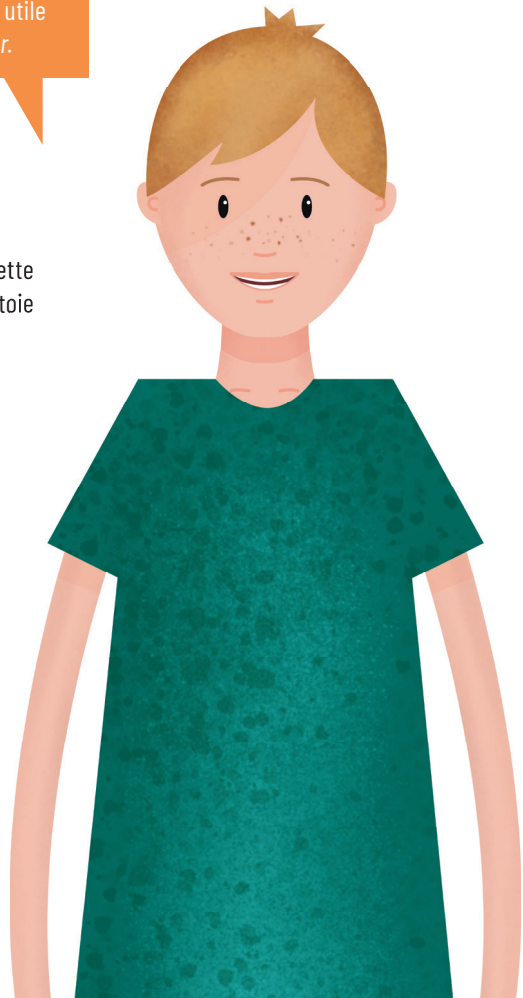
Chapitre 3

Chasse aux virus

Pour supprimer les virus, il faut cliquer dessus. Cette opération est répétée dans tout le menu. Cela nettoie la tablette des virus.

Chasse aux virus RA

Une grille apparaît. L'application doit, avec l'aide de la caméra, détecter une surface aussi plane et structurée que possible (murs, sols, tables, etc.). Si cela ne fonctionne pas tout de suite, continue à chercher des surfaces plus adaptées. Il faut parfois changer de pièce ou modifier l'éclairage pour que la caméra puisse reconnaître une surface suffisamment structurée. Après cela, le mini-jeu commence. Dans ce jeu RA, il faut lancer un logiciel antivirus sur les virus. Pour ce faire, appuie longuement ou de manière



répétée sur le bouton avec l'icône du viseur. Tu définis la direction en déplaçant la tablette. Les virus apparaissent par étapes dans toute la pièce. L'ennemi final (supervirus) doit être touché plusieurs fois pour être désactivé et capturé.

Jeux analogiques à faire entre-deux

Carte *KryptoKids*

Matériel nécessaire

- Document téléchargeable, papier, ciseaux, épingles de sûreté

Le fichier pour la carte *KryptoKids* peut être téléchargé et imprimé. Les participant·e·s peuvent ensuite décorer leur propre carte et l'attacher à leur haut avec une épingle à nourrice.

Terrier

Matériel nécessaire

- Chaises pour un cercle de chaises (une de moins que le nombre de participant·e·s).

Comme dans le jeu connu de la salade de fruits, les enfants sont assis en cercle sur des chaises. Un·e volontaire au milieu révèle maintenant quelques informations sur sa personne (par exemple : « J'ai mangé des céréales ce matin », « J'ai deux frères et sœurs », « J'aime jouer de la guitare »). Chaque personne du cercle à laquelle cette information s'applique également doit maintenant changer de place le plus rapidement possible. La personne volontaire qui était debout au départ essaie elle aussi de s'asseoir sur une des chaises qui se sont libérées. L'enfant qui se retrouve sans chaise continue le jeu.

Pédagogie sous-jacente :

- Réflexion : partage d'informations personnelles.
- Ces informations pourraient-elles être utilisées contre vous ?
- Partageriez-vous cette information même si vous ne connaissiez pas les autres participant·e·s ?
- Avez-vous gardé volontairement certaines informations pour vous ?
- Transition entre informations privées et informations publiques.

Je protège mes données

Tous les participant·e·s s'assoient en cercle. La première personne commence par la phrase « Je protège mes données et je protège … ! » et ajoute quelque chose qu'elle ne révélerait pas sur internet. Par exemple : « Je protège mes données et je protège mon nom de famille ! » Ensuite, la personne suivante doit répéter la phrase et ajouter un autre mot. Exemple : « Je protège mes données et je protège mon nom de famille et mon lieu de résidence ! ». Le jeu continue ainsi. La personne qui ne peut plus rien ajouter ou fait une erreur au niveau de l'ordre de ce qui a été énuméré a perdu.

Pédagogie sous-jacente :

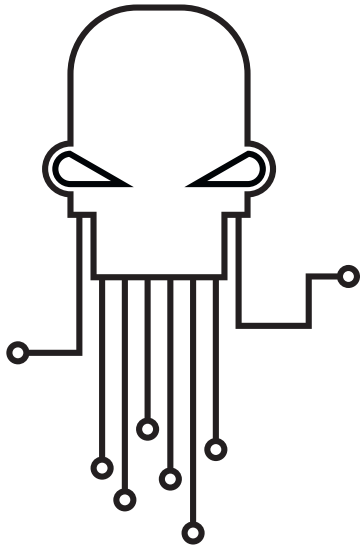
- Réflexion : quelles sont les données qui méritent d'être protégées ?
- Entraînement de la mémoire

Chasse aux *DataPieuvs*

Matériel nécessaire

- un flip-chart ou un tableau noir
- des stylos ou des craies

La chasse aux *DataPieuvs* est basée sur le célèbre jeu du pendu. On choisit une personne qui pense à un mot aussi long que possible sur le thème de la protection des données, la sécurité des données, internet, etc. Cette personne trace le nombre de lettres que le mot a sous forme de lignes horizontales les unes à côté des autres. Les autres joueurs et joueuses peuvent maintenant nommer tour à tour une lettre. Si une lettre est devinée correctement, elle est inscrite à l'endroit approprié. Si une lettre est mal devinée, une partie de la pieuvre est dessinée. D'abord la tête, puis les yeux et l'un après l'autre les huit tentacules.



Le but du jeu est de deviner le mot avant que l'image de la pieuvre ne soit complète.

Problèmes éventuels et FAQ

L'intro est terminée. Qu'est-ce que je dois faire maintenant ?

Dans le menu de la barre latérale gauche, tu trouves tous les outils dont tu as besoin pour retrouver les *DataPieuvs*. Pour pouvoir commencer, il faut que tu regardes une fois tout le menu. Dans la boîte de réception de ton programme de courrier électronique, tu trouves encore une fois toutes les informations relatives à l'affaire. Tu peux aussi y regarder une nouvelle fois la vidéo de la présentatrice du journal télévisé.

Qu'est-ce que je peux faire lorsque des termes ne sont pas clairs pour moi ?

Si tu ne connais pas un terme technique, tu peux le chercher dans le wiki. Tous les mots étrangers y sont expliqués de manière simple. Si cela ne suffit pas, pose la question à une personne de référence.

J'ai des problèmes avec le *KryptoScanner*. Que faut-il faire ?

Si tu as trouvé un classeur, tu dois scanner l'étiquette du classeur avec le *KryptoScanner*. C'est la seule façon d'accéder aux données du dossier. Lorsque tu scannes, tu devrais t'éloigner d'un pas ou deux de l'étiquette. Ensuite, le *KryptoCube* apparaît.

Le *KryptoCube* ne s'emboîte pas. À quoi cela est-il dû ?

Si le *KryptoCube* ne s'emboîte pas, c'est que tu ne l'as pas encore mis dans la bonne position. Appuie sur la flèche pour faire tourner le cube. Tu dois faire pivoter le cube jusqu'à ce que, vu du dessus, il ressemble exactement à l'étiquette du classeur. Là le cube s'emboîte.

Je n'arrive pas à attraper les triangles volants. Qu'est-ce que je fais comme erreur ?

Si les triangles ne sont pas collectés, c'est généralement parce que le *KryptoScanner* a perdu de vue l'étiquette du classeur. Veille à ce que l'étiquette reste toujours visible dans le scanner. Tu peux aussi essayer de modifier la distance par rapport au classeur et voir si cela fonctionne mieux. En haut à droite, tu vois un petit triangle qui t'indique le nombre de triangles qu'il te reste à attraper.

L'application est bloquée. Qu'est-ce que je peux faire ?

La meilleure chose à faire est de quitter l'application et de la redémarrer. Cliquer deux fois de suite sur le bouton accueil de la tablette (bouton rond en bas au milieu) et faire glisser l'application vers le haut pour l'éjecter.

Personnes et acteurs impliqués

Équipe fjmk :	Birgit Schlotter, Felix Dietz, Karolina Albrich, Maren Kirsch, Markus Sindermann, Saskia Moes
Équipe GLUON STUDIOS :	Arzu Uyan, Eckhard Seidel, Remus Constantin, Sandro Vilusic, Stephan Klefisch
Équipe Jugendarbeit.digital (Suisse) :	Eike Rösch, Rafael Freuler
Conception graphique :	Ulrike Beck
Voix *KryptoKids (en allemand)* :	Schauspielschule & Stageschool Salomon Academy: Amalia Bachmann, Antonia Reichel, Katharina Kugelmeier, Lisa Maria Ohl, Robin Schleifenbaum, Stefan Goldberg
Voix *KryptoKids (en français)* :	Aurélie Cuvelier Favier, Gaïa Samakh, Kevin Ouadhi, Maéva Napen, Maxime Moreau, Sophia Fabian
Conception sonore :	Sascha Haus
Soutien texte :	Andreas Gloge
Photos :	Jan Faßbender
Traduction française :	Marilène Broglie

Publié par la Fachstelle für Jugendmedienkultur NRW et GLUON STUDIOS, Édition 2021

Le guide *KryptoKids* 2021 de la Fachstelle für Jugendmedienkultur NRW und GLUON STUDIOS est couvert par une licence Creative Commons Paternité – partage à l'identique 4.0 licence internationale (CC-BY-SA 4.0).

Sources

Baacke, Dieter. 1997. Medienpädagogik. Grundlagen der Medienkommunikation. Tübingen.

Un projet commun de :

fjmk Fachstelle für Jugendmedienkultur NRW

Fachstelle für Jugendmedienkultur NRW
Weinsbergstr. 190
50825 Köln
Allemagne

www.fjmk.de

GLUON STUDIOS GmbH
Marienstr. 71
50825 Köln
Allemagne

www.gluonstudios.com

***KryptoKids* Suisse :**

Jugendarbeit.digital

Jugendarbeit.digital
Wartstrasse 5
8400 Winterthur
Suisse

www.jugendarbeit.digital

Avec le soutien de :

STIFTUNG DEUTSCHE JUGENDMARKE e.V.

MANAWA FOUNDATION

JEUNES ET MÉDIAS
PLATEFORME NATIONALE DE PROMOTION DES COMPÉTENCES MÉDIATIQUES

Contacter les *KryptoKids* :

Allemagne : Fachstelle für Jugendmedienkultur NRW · info@krypto-kids.de · www.krypto-kids.de
Suisse : Jugendarbeit.digital · info@krypto-kids.ch · www.krypto-kids.ch