ACTIVITÉ 4 · SI · 7e

SÉCURITÉ DES ACCÈS INFORMATIQUES

<DÉ>CODAGE • ÉDUCATION NUMÉRIQUE • CYCLE 2 (7e-8e)
DEF-DGEO (VAUD, SUISSE)
2023 • DECODAGE.EDU-VD.CH • CC BY NC SA 4.0

PLAN D'ÉTUDES ROMAND

EN 22 — S'approprier les concepts de base de la science informatique…

2 … en encodant, décodant et en transformant des données

3 … en utilisant différentes machines et en découvrant le fonctionnement des réseaux

Information et données

Découverte des différents types de fichiers permettant de représenter des informations

Machines, systèmes, réseaux

Identification des composants principaux *(processeur, mémoire, dispositifs d'entrée/sortie, …)* de différents types de machines *(ordinateur, tablette, robot, …)* et de leurs fonctions

Découverte de techniques simples de sécurité de systèmes informatiques

Liens disciplinaires

MSN 24 – Grandeurs et mesures
SHS 21 – Relation Homme-Espace

INTENTIONS PÉDAGOGIQUES

Le but de cette activité est double :

- comprendre l'importance des données privées d'une personne ou provenant du monde du travail, et la nécessité d'en protéger l'accès contre des personnes extérieures ou des systèmes informatiques ;
- découvrir les différentes méthodes de protection contre l'accès à ces données sur un ordinateur ou un téléphone.

DESCRIPTION DE L'ACTIVITÉ

Cette activité se déroule sur deux séances :

Séance 1 (45 minutes) :

On débute en proposant une réflexion sur la nécessité de protéger des données numériques, à travers deux exemples et à l'aide de questions-réponses avec les élèves.
Puis, sont présentées deux méthodes pour accéder à un compte informatique, en ligne ou en local : l'authentification par nom et mot de passe ainsi que la double authentification.

Ensuite, trois méthodes sont décrites pour accéder à un smartphone : mot de passe, modèle de chemin et biométrique.

Séance 2 (45 minutes) :

Elle débute par un temps consacré à l'élaboration d'un mot de passe sûr. La présentation du chiffrage de fichiers est abordée. Finalement, l'attaque par hameçonnage (phishing) est analysée.

Prérequis :

Activité de 6e, « Se connecter à un site protégé ».

DONNÉES PERSONNELLES ET CONFIDENTIALITÉ

Cette activité permet d'aborder la notion de données personnelles ou d'intérêt général et de leur confidentialité. Afin d'outiller le corps enseignant dans l'explication de certaines notions, les indications pédagogiques sont ponctuées d'encarts faisant à la fois office d'éclairage théorique et d'éléments.

Séance 1 - Pourquoi et comment protéger les accès aux données sur un ordinateur ou en ligne ?

MODALITÉ	En collectif
MATÉRIEL	• Fiche 1 : connexion par mot de passe et CAPTCHA • Fiche 2 : authentification et site web • Fiche 2.1 : authentification et site web « corrigé » • Fiche 3 : caractéristiques des méthodes de connexion • Fiche 3.1 : caractéristiques des méthodes de connexion « corrigé » • Affichage numérique • Ordinateur pour la classe
DURÉE	45 minutes

TEMPS 1.1 — LES SECRETS DE SACHA — 15 minutes

UN PREMIER EXEMPLE :

Depuis longtemps déjà, Sacha a pris l'habitude de tenir un petit cahier dans lequel il ou elle note ses événements journaliers, des commentaires sur ses amies et amis, ses mouvements d'humeur, gais comme tristes, ses désirs secrets, etc. Depuis que son frère lui a dérobé son cahier pour s'amuser, Sacha ne sait plus où le cacher dans la maison. Aussi Sacha a décidé de le recopier et de le conserver sur un ordinateur...

A. « Une fois copié sur un ordinateur, le cahier de Sacha est-il en sécurité ? Que peut-il se passer ? »

Réponses possibles : quelqu'un qui accéderait à l'ordinateur pourrait peut-être lire le cahier. Ou pire, modifier son contenu ou même l'effacer. Sacha souhaite évidemment que son contenu reste privé. Plus d'informations sur les données personnelles via ce lien *78-S3-22*.

B. « Savez-vous sous quelle forme est conservé le cahier sur l'ordinateur ? »

Réponse : le cahier est conservé sous forme d'un **fichier** (voir définition dans l'encadré ci-dessous) rangé dans un **support de stockage** de l'ordinateur.

MODULARITÉ

FICHIER ET SUPPORT DE STOCKAGE

Un support de stockage est un dispositif matériel qui conserve des données de manière permanente (à moins qu'un système ne les modifie). Exemples : carte mémoire SSD, disque dur, clé USB.

Un fichier est un enregistrement de données sur un support de stockage, repéré par un nom.

Ces données peuvent être du texte, des sons, des images, etc. Il existe aussi des données inaccessibles aux humains et destinées à être utilisées seulement par une machine.

UN SECOND EXEMPLE :

La petite société ÉnergiePlus vient d'inventer un moteur de voiture révolutionnaire non polluant, facile à fabriquer et ne consommant pas de pétrole.

C. « Aurait-elle intérêt à garder secrète sa technique de fabrication ? Pour quelle raison ? »

Réponse : oui, si cette petite société souhaite vendre sa nouvelle invention, elle doit protéger son idée et donc garder le secret. Car une autre société, plus puissante, pourrait lui dérober les documents de fabrication, produire et vendre les nouveaux moteurs, gagner beaucoup d'argent, au détriment d'ÉnergiePlus.

On peut compléter ces deux exemples par la liste suivante :

- protection contre l'accès par des personnes ou par des systèmes extérieurs aux comptes privés dans un réseau d'école, d'entreprise, etc. ;
- protection de sites internet commerçants contre le vol de données relatives aux clients (identifiants, adresse mail, numéro de cartes bancaires, etc.) ;
- protection du dossier médical d'un patient chez le médecin ou à l'hôpital, contre une intrusion de la presse par exemple ;
- protection des échanges sur les réseaux sociaux contre des personnes qui voudraient diffuser à tout le monde le contenu de conversations ;
- protection des identifiants bancaires des personnes contre des attaques passant par Internet ;
- protection des installations militaires d'un pays contre les nations étrangères qui se livreraient à de l'espionnage.

TEMPS 1.2 — PROTÉGER L'ACCÈS À UN COMPTE — 15 minutes

CONNEXION SIMPLE (RAPPEL) :

Dans l'activité proposée en 6e, « Se connecter à un site protégé », les notions de données personnelles ainsi que l'accès à un compte privé par le réseau informatique d'une école ont été étudiés.

Un rappel du connu est présenté ici sous forme de questions pour les élèves ayant fait cette activité, une petite remise en contexte est souhaitée pour les élèves n'ayant pas vu cette activité.

Afficher la *Fiche 1* et poser aux élèves les questions suivantes :

A. « Quel mot se trouve à la place du rectangle 1 ? »

Réponse : nom (identifiant ou login sont aussi acceptés).

B. « Quel mot se trouve à la place du rectangle 2 ? »

Réponse : mot de passe.

C. « Par quel mot appelle-t-on les informations à saisir dans le repère 3 ? »

Réponse : les identifiants, les éléments de connexion ou plus familièrement les codes.

D. « Comment s'appelle la figure du repère 4 ? »

Réponse : un CAPTCHA. Il s'agit d'une famille de tests permettant de différencier de manière automatisée un utilisateur humain d'un ordinateur. Ce test est utilisé en informatique pour vérifier que l'utilisateur n'est pas un robot textuel.

E. « Que se passe-t-il si on clique sur le bouton "Valider" (repère 5) ? »

Réponse : si les deux champs du repère 3 sont correctement remplis ainsi que les sélections dans le CAPTCHA, l'utilisateur est authentifié, sa session s'ouvre, donnant accès à son contenu privé.

DOUBLE AUTHENTIFICATION

Imaginons maintenant que les identifiants d'un utilisateur d'un site web de commerce soient volés par une personne malveillante. Ce pirate va alors pouvoir se connecter à la place de l'utilisateur, la confidentialité de son compte n'est donc plus assurée. Le CAPTCHA n'apporte aucune protection, puisque le pirate peut le remplir correctement. Pour renforcer l'authenticité de l'utilisateur, on fait appel à la double authentification.

Lors de la connexion, en plus du nom et du mot de passe, une demande de confirmation est envoyée à l'utilisateur par un moyen indépendant.

Par exemple, le système d'authentification envoie à l'utilisateur, propriétaire du compte, un courrier électronique (e-mail) qui contient un nombre. L'utilisateur prend connaissance du nombre et le tape dans une zone réservée de la page d'authentification.
Le nombre peut être également communiqué par un SMS sur son téléphone.

Un pirate ne recevra pas l'e-mail ou le SMS. Il ne pourra pas confirmer son identité, et sa tentative de connexion échouera.

Ce mécanisme s'appelle la **double authentification ou authentification à deux facteurs** car il comprend :

- une première authentification par les identifiants ;
- une seconde authentification par le moyen de confirmation.

Sur la *Fiche 2* les élèves relient les situations présentées au mode d'identification le plus adapté.

« Pour résoudre ces situations, on se met à la place de quelqu'un qui se connecte sur un ordinateur (fixe, portable, tablette). »

Le corrigé se trouve sur la Fiche 2.1.

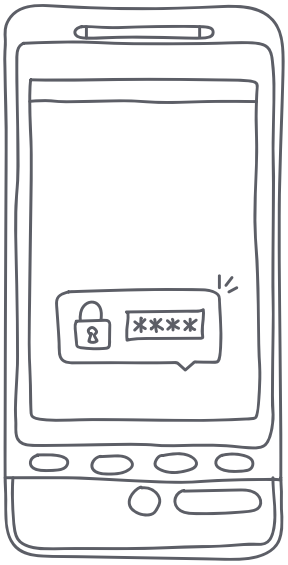
TEMPS 1.3 ACCÉDER À UN TÉLÉPHONE MOBILE PROTÉGÉ 15 minutes

« Comment se passe l'authentification de l'utilisateur d'un téléphone mobile ? »

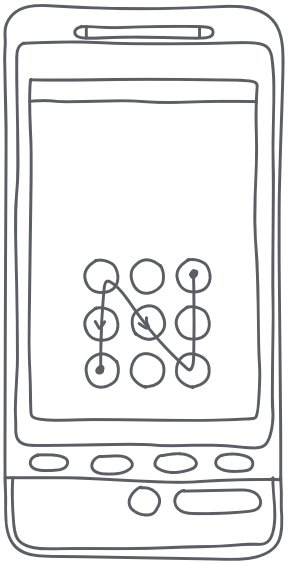
MODULARITÉ

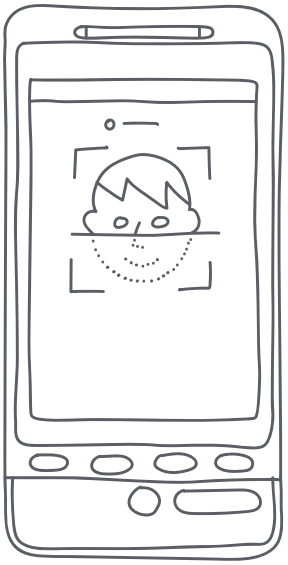
AUTHENTIFICATION SUR UN TÉLÉPHONE MOBILE

Un téléphone mobile accepte un seul utilisateur identifié. Cette information n'est pas détenue par le téléphone mais dans une petite carte, appelée carte SIM, fournie par l'opérateur téléphonique de l'utilisateur.
Une partie de l'authentification est donc déjà faite. Il y a ensuite une autre authentification, celle du smartphone lui-même. La méthode pour le faire peut prendre des formes variées. Par exemple :



Identification par mot de passe


Identification par modèle de chemin


Identification biométrique

- L'identification par **mot de passe** est bien connue. Elle fera l'objet d'un temps spécifique à la fin de cette activité.
- L'identification par **modèle de chemin** consiste à dessiner un modèle (ou motif) géométrique en reliant des points disposés sur l'écran tactile du téléphone.
- L'identification **biométrique** consiste à reconnaître l'utilisateur par une de ses caractéristiques physiques ou comportementales :
  - l'empreinte digitale d'un doigt ou un scan de la main ;
  - une partie de l'œil comme la rétine ou l'iris ;
  - le visage (reconnaissance faciale) ;
  - la voix (reconnaissance vocale).

« Toutes ces méthodes d'authentification se valent-elles ou certaines sont-elles plus adaptées que d'autres selon les situations ? Sur la *Fiche 3*, reliez les caractéristiques à la méthode d'identification la plus adaptée. Il peut y avoir plusieurs liens qui partent du même endroit ou arrivent au même endroit. »

Corriger collectivement à l'aide de la Fiche 3.1.

Séance 2 - Acquérir des compétences pour mieux se protéger (mot de passe, hameçonnage)

MODALITÉ	En collectif
MATÉRIEL	• Fiche 4 : exemples de temps de recherche de mot de passe • Fiche 4.1 : exemples de temps de recherche de mot de passe « corrigé » • Fiche 5 : chiffrage d'un texte • Fiche 6 : exemple de hameçonnage • Fiche 6.1 : exemple de hameçonnage « corrigé » • Fiche 7 : glossaire et conseils • Affichage numérique • Ordinateur pour la classe
DURÉE	45 minutes

TEMPS 2.1 — MOT DE PASSE — 15 minutes

DES MOTS DE PASSE CONNUS

Le mot de passe est la méthode la plus connue pour contrôler l'accès à une ressource (ordinateur, site web, fichier, etc.).

Un mot de passe est composé de caractères : des chiffres, des lettres (en majuscules et/ou en minuscules) et des caractères spéciaux (par exemple : &, ?, #, !, etc.).

« Souvent le mot de passe est inventé ou choisi par un utilisateur qui veut protéger un accès. Comment l'utilisateur va-t-il choisir son mot de passe ? Faisons une expérience. »

L'enseignante ou l'enseignant choisit un mot de passe d'un seul caractère qui est obligatoirement un chiffre et la classe doit le deviner.

A. « Qui propose un chiffre pour deviner mon mot de passe ? »

Réponse : rapidement, au bout de quelques tentatives, le mot de passe est trouvé. Les élèves conviennent que le choix n'est pas efficace car ils ont une chance sur dix de découvrir le mot de passe. Il suffit de répéter l'essai.

B. « Proposer une petite amélioration pour que le mot de passe soit plus difficile à deviner. »

Voici ici trois propositions de réponses d'élèves, les relancer chaque fois avec une question.

1) Utiliser deux chiffres au lieu d'un.

« Si quelqu'un essaie de découvrir mon mot de passe, il a une chance sur combien d'y arriver ? »

Réponse : 10 x 10 = 100 car il y a 100 nombres (entiers) à 2 chiffres de 00 à 99. Donc 1 chance sur 100.

2) Utiliser une lettre au lieu d'un chiffre.

« Si quelqu'un essaie de découvrir mon mot de passe, il a une chance sur combien d'y arriver ? »
Réponse : il y a 52 possibilités (en comptant les 26 majuscules et les 26 minuscules). Donc 1 chance sur 52.

3) Utiliser un caractère qui peut être une lettre ou un chiffre.
« Si quelqu'un essaie de découvrir mon mot de passe, il a une chance sur combien d'y arriver ? »
Réponse : il y a 62 possibilités (il faut ajouter 10 chiffres au 52 lettres). Donc 1 chance sur 62.
Certains élèves peuvent penser que c'est suffisant car ils risquent d'oublier que l'on peut faire plusieurs essais.

C. « On cherche à deviner le mot de passe. Comment imaginez-vous procéder ? »

Réponse probable : on essaie plusieurs fois, au hasard.

D. « Si on fait un grand nombre d'essais, comment être sûr de ne pas répéter les mêmes essais ? »

Réponse : on passe en revue toutes les combinaisons de manière ordonnée, par ordre croissant, par exemple. Avec suffisamment d'essais, on est sûr de tomber sur le mot de passe. Cette technique simple s'appelle le décryptage par force brute.

Livrons-nous à quelques calculs élémentaires. Imaginons un système qui tente de forcer un mot de passe, avec 1 000 000 d'essais par seconde. Cette vitesse de test est à la portée d'un ordinateur classique, à condition que rien ne vienne le ralentir.

Pour le mot de passe, supposons que chaque caractère puisse être un chiffre, une lettre majuscule ou minuscule, ou un caractère spécial (on peut en trouver une quarantaine sur le clavier d'un ordinateur).

Il y a donc 10 (chiffres) + 26 (majuscules) + 26 (minuscules) + 40 (caractère spéciaux) = 102 caractères. Arrondissons à 100 caractères.

On demande alors aux élèves de compléter le tableau de la *Fiche 4*, en s'aidant de la calculatrice (pour la colonne 3). Ils expriment les durées de temps en jours, mois, années, si nécessaire.

ENVIRONNEMENT SOCIO-TECHNIQUE

LE DÉCRYPTAGE (OU ATTAQUE) PAR FORCE BRUTE

Il consiste à essayer toutes les combinaisons possibles jusqu'à trouver la bonne. C'est la méthode la plus simple, qui est certaine d'aboutir, mais pouvant être longue.

Plus le mot de passe est long, plus le temps pour le trouver l'est également. On voit ainsi l'intérêt de choisir un mot de passe à plusieurs caractères et le plus varié possible.

En réalité, les gens non avertis ont tendance à choisir des mots de passe faciles à retenir, comme une date de naissance, un prénom, un objet, etc.

E. « D'après vous, quels sont les mots de passe les plus utilisés ? »

DES MOTS DE PASSE CONNUS

Les mots de passe les plus utilisés en Suisse sont :

- 123456
- 123456789
- 12345
- password
- 12345678
- 1234
- qwerty ou qwertz

(source Nordpass)

Certaines attaques commencent par tester les mots de passe courants. Elles essaient aussi tous les mots de la langue (200'000 mots en français). Il s'agit d'une attaque par dictionnaire.

F. « Proposez un mot de passe en expliquant comment vous l'avez choisi. »

Réponse possible : il peut être trop simple ou trop commun, mais certains élèves choisiront des mots de passe compliqués. Leur faire alors comprendre qu'ils seront également difficiles à retenir.

QUELQUES CONSEILS SUR LES MOTS DE PASSE

- Ne pas utiliser de dates, de prénoms ou de diminutifs, ou encore un mot de la langue du pays ou en anglais.
- Créer un mot de passe d'au moins 8 caractères contenant des lettres (majuscules et minuscules), des chiffres et des symboles.
  La tendance actuelle consiste à utiliser une phrase de texte. On a alors un mot de passe qui contient beaucoup de caractères, donc difficile à décrypter tout en étant facile à retenir.
- Pour chaque accès à protéger, créer des mots de passe différents.
- Lorsque l'on a beaucoup de mots de passe, il est possible d'utiliser un logiciel coffre-fort.
  Ce programme contient tous les mots de passe ; le seul à retenir est celui permettant d'ouvrir le coffre-fort.
- Éviter d'écrire le mot de passe quelque part.

Nous avons vu que le mot de passe permet de protéger l'accès à un système informatique.
On peut également l'utiliser pour protéger l'accès au contenu d'un fichier ou d'un dossier.

TEMPS 2.2 CHIFFRER LES FICHIERS ET LES DOSSIERS 10 minutes

« Imaginons que malgré tout, une personne ou une machine accède à vos données. Comment s'assurer qu'elle ne pourra pas les lire ou les comprendre ? »

LE CHIFFRAGE

On protège les fichiers qui contiennent des informations confidentielles, pour cela, un logiciel qui chiffre les données est utilisé. Le **chiffrage** consiste à modifier ces données pour les rendre illisibles. Cette transformation est réversible, de sorte que l'on peut rendre à nouveau les données lisibles en les **déchiffrant**. Chiffrage et déchiffrage sont effectués par des logiciels spécialisés. Pour autoriser une personne à chiffrer ou déchiffrer un fichier, la pratique la plus courante consiste à utiliser un mot de passe.

« Jusqu'à maintenant, nous avons vu comment protéger l'accès à des ordinateurs, en direct ou à distance par Internet. D'après vous, est-ce utile de pouvoir chiffrer des fichiers ? »

Exemple : créons le petit fichier appelé **exemple-chiffrage.txt** qui contient le texte « Le ciel est bleu ».

On peut visualiser, avec un logiciel adapté, comment se présente le texte une fois stocké dans le support de stockage (afficher la *Fiche 5*).

Préciser éventuellement aux élèves que le codage utilisé pour coder la phrase est le système hexadécimal, qui sera vu au degré secondaire (image 1).

Puis, on chiffre le fichier en utilisant le mot de passe **Ay4&r** (image 2).

Un nouveau fichier est créé, voyons ce qui se trouve dedans (image 3).

Dans les données lisibles, on retrouve le nom du fichier qui lui est en **clair**, ce qui est normal puisque il n'est pas à cacher. Mais on ne voit plus la phrase « Le ciel est bleu », elle est chiffrée et inaccessible à qui n'est pas autorisé.

MÉTHODE DE CHIFFRAGE AES-256

La méthode de chiffrage utilisée dans l'exemple précédent se nomme AES-256, c'est une méthode sûre, qui utilise un algorithme complexe.
Les méthodes de chiffrage progressent en permanence car elles doivent résister à des attaques qui évoluent également et qui deviennent de plus en plus sophistiquées.

Il existe aussi des logiciels qui permettent de chiffrer de grand volume de dossiers et de fichiers. L'accès se fait via un mot de passe.

TEMPS 2.3 | HAMEÇONNAGE (« PHISHING » EN ANGLAIS) | 15 minutes

« Jusqu'à présent, nous avons vu comment protéger l'accès à ses données, comment les chiffrer pour ne pas les rendre lisibles. Mais il y a d'autres manières d'accéder à vos informations. Avez-vous une idée ? »

La réponse attendue est : **« En vous demandant directement vos informations ! C'est culotté et bien sûr cela se fait de manière déguisée. Cela s'appelle le hameçonnage ou "phishing" en anglais. Savez-vous comment cela se présente ? »**

LE HAMEÇONNAGE

Le hameçonnage est une méthode utilisée par des fraudeurs pour obtenir d'une victime, des informations personnelles (mots de passe, numéros de carte bancaire ou de carte d'identité, etc.), en faisant croire que la demande vient de personnes de confiance (administration, banque, etc.).

« Comment les fraudeurs prennent-ils contact avec les victimes ? »

Dans la majorité des cas, le hameçonnage se manifeste par un courrier électronique ou un SMS dont le but est de faire réagir la victime pour qu'elle suive les instructions qui lui sont présentées.

« Quels sont les motifs qui font réagir les lecteurs d'un mail de hameçonnage ? »

- La convoitise, par exemple, en proposant un gain d'argent ou un cadeau.
- La peur, en proférant des menaces : « Votre compte sera fermé si ... » ou « Nous publierons les photos ... ».
- La bonté, en voyage à l'étranger, une connaissance a de gros soucis et vous demande de l'aide (une somme d'argent).
- Il inspire la confiance, il feint d'être envoyé par une source sûre ou institutionnelle (l'administration des impôts, la police, une société internationale, une de vos connaissances, etc.).

Il est alors proposé de se connecter sur un site web. Sous un prétexte qui paraît possible mais qui est en réalité faux, des informations sensibles : les coordonnées personnelles, le numéro de téléphone, les coordonnées bancaires, le numéro de carte de crédit, les identifiants divers sont demandées. Une fois ces informations volées, la personne malveillante peut les utiliser à son profit, par exemple pour obtenir de l'argent.

« Comment savoir si le courrier est du hameçonnage ou s'il est authentique ? Comment s'en protéger ? »

En étant méfiant et observateur. Qu'il s'agisse d'un courrier électronique ou d'un site web, avant d'avoir déterminé s'il est digne de confiance :

- ne cliquer sur aucun lien, ne pas ouvrir les pièces jointes ;
- vérifier que le message mentionne votre nom ;
- il doit être rédigé en bon français ;
- ne communiquer aucune information personnelle ;
- l'émetteur doit être crédible (si c'est une personne, être sûr de la reconnaître. S'il s'agit d'une organisation, vérifier sur le web ses dénominations).

Exemple :
On distribue ou on projette les deux courriers électroniques de la *Fiche 6*.

« À la lecture attentive de ces deux courriers, déterminez celui qui est frauduleux. Expliquez les raisons précises de votre méfiance. »

Les erreurs d'orthographe du message 1 sont intentionnelles. Le corrigé se trouve sur la Fiche 6.1.

TEMPS 2.4	INSTITUTIONNALISATION	5 minutes

Distribuer la *Fiche 7* et effectuer une lecture interactive en répondant aux questions des élèves.
Ici l'enseignante ou l'enseignant pose et explicite les savoirs de la séance.

Connexion par mot de passe et CAPTCHA

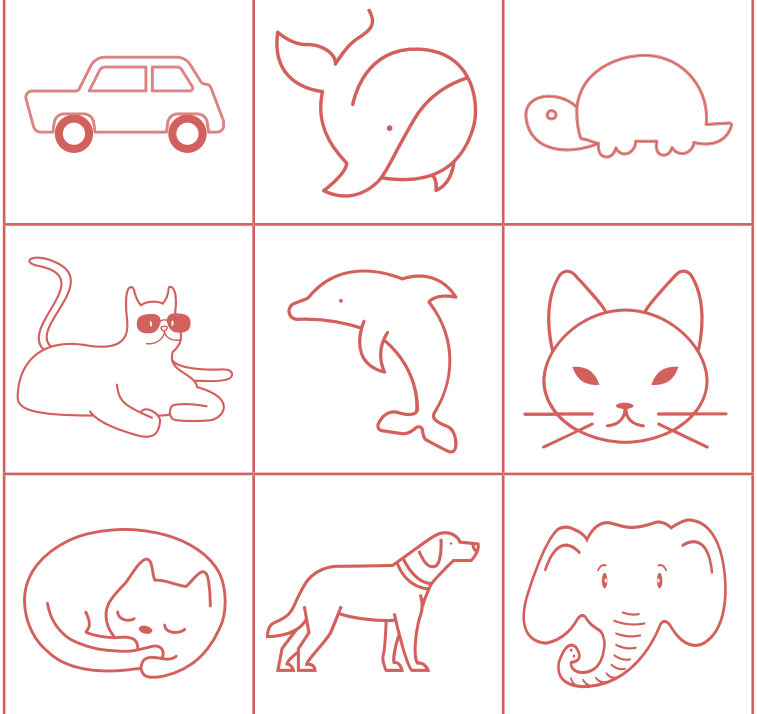
Bienvenue !

1 3

2

ÊTES-VOUS UN ROBOT ?

4 **CLIQUER SUR TOUS LES CHATS**



OK

5 **VALIDER**

Authentification et site web

Relie chaque situation au bon mode d'identification.

Connexion...

- **... à un site de météo.** ●
- **... à mon compte sur le site de la banque.** ●
- **... à mon compte sur le site de l'école.** ●
- **... à mon compte sur un site de vente de vêtements.** ●
- **... à Wikipédia.** ●
- **... à mon compte sur le site des impôts.** ●
- **... à mon compte sur un site de musiques gratuites (payé par la publicité).** ●

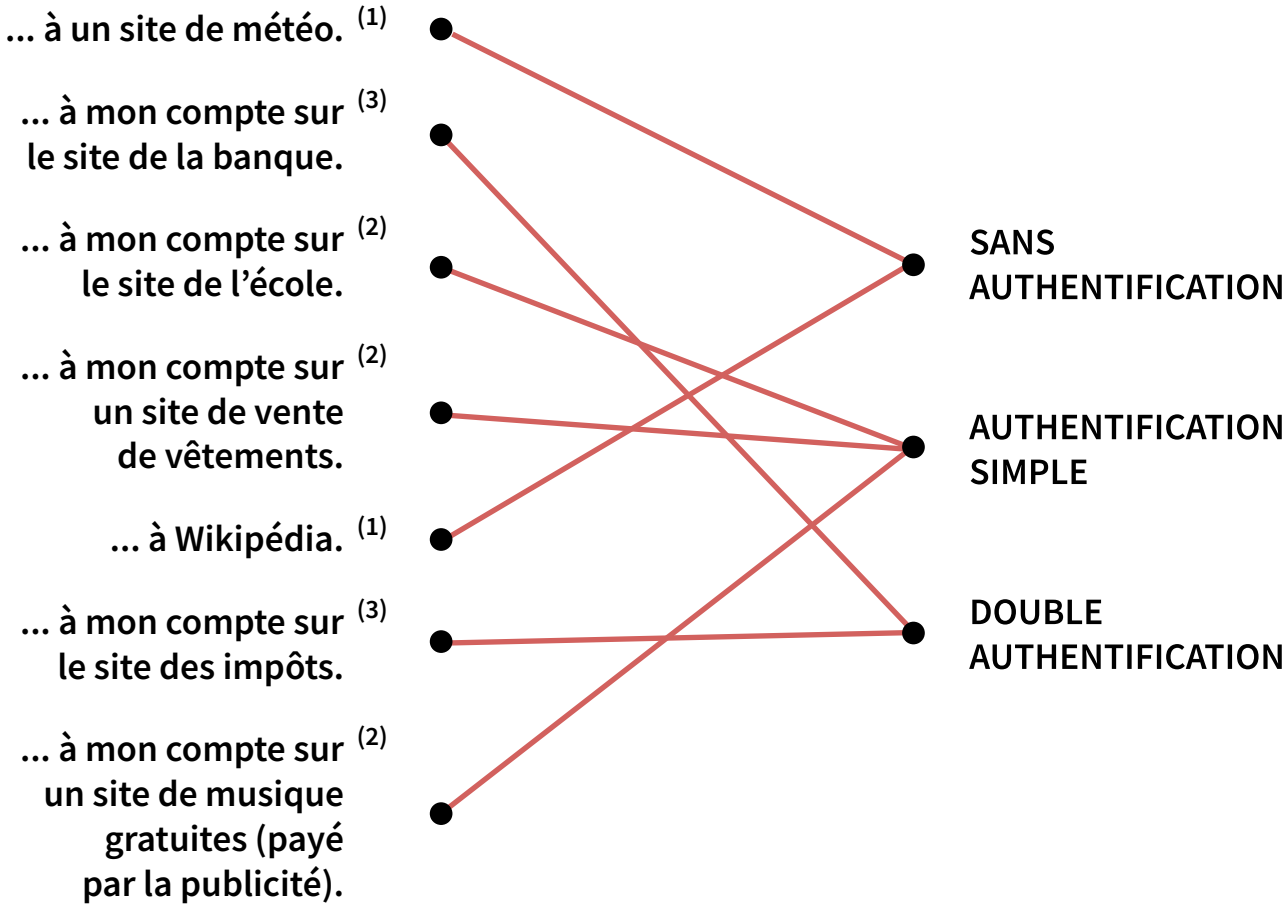
- ● **SANS AUTHENTIFICATION**
- ● **AUTHENTIFICATION SIMPLE**
- ● **DOUBLE AUTHENTIFICATION**

CORRIGÉ

Authentification et site web

Relie chaque situation au bon mode d'identification.

Connexion...



COMMENTAIRES :

1. Pour des sites comme Wikipédia ou la météo, les données sont publiques, tout le monde peut y avoir accès, nul besoin de prouver son identité.
2. Pour le site de musique, pas de risque de fraude donc une authentification simple suffit.
   Pour l'école, l'utilisateur n'a pas de téléphone ou de dispositif accessible pour lire un e-mail.
   Pour le site de vêtements, le vendeur pense probablement qu'une authentification trop compliquée risque de rebuter le client.
3. Le site des impôts ou de la banque recèle des informations privées dites « sensibles », informations liées à la situation financière de l'utilisateur.

Caractéristiques des méthodes de connexion

Relie chaque caractéristique à la bonne méthode de connexion.

Connexion qui...

- **... fait intervenir la mémoire.**
- **... est assez rapide.**
- **... est spécifique à chaque personne.**
- **... mal gérée, peut être facile à usurper.**
- **... est incopiable.**
- **... est la plus ancienne.**
- **... n'est pas proposée par tous les téléphones.**

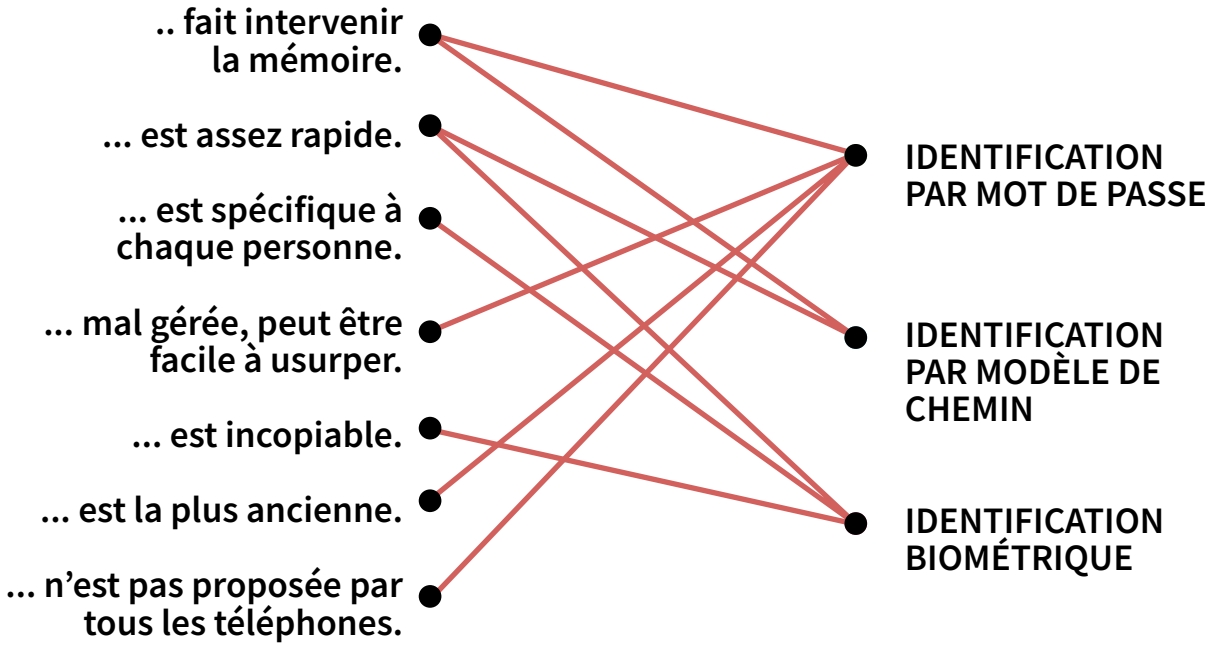
- **IDENTIFICATION PAR MOT DE PASSE**
- **IDENTIFICATION PAR MODÈLE DE CHEMIN**
- **IDENTIFICATION BIOMÉTRIQUE**

CORRIGÉ

Caractéristiques des méthodes de connexion

Relie chaque caractéristique à la bonne méthode de connexion.

Connexion qui...



Exemples de temps de recherche de mots de passe

Complète ce tableau.

NOMBRE DE CARACTÈRES	NOMBRE DE COMBINAISONS	TEMPS DE RECHERCHE MAXIMAL
1	100	100 / 1 000 000 = 0,0001 s
2		
8		
12		

Complète ce tableau.

NOMBRE DE CARACTÈRES	NOMBRE DE COMBINAISONS	TEMPS DE RECHERCHE MAXIMAL
1	100	100 / 1 000 000 = 0,0001 s
2		
8		
12		

Complète ce tableau.

NOMBRE DE CARACTÈRES	NOMBRE DE COMBINAISONS	TEMPS DE RECHERCHE MAXIMAL
1	100	100 / 1 000 000 = 0,0001 s
2		
8		
12		

CORRIGÉ

Exemples de temps de recherche de mots de passe

Complète ce tableau.

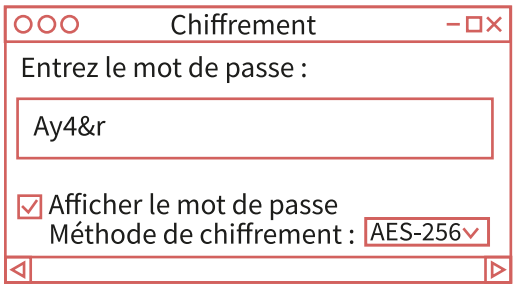
NOMBRE DE CARACTÈRES	NOMBRE DE COMBINAISONS	TEMPS DE RECHERCHE MAXIMAL
1	100	100 / 1 000 000 = 0,0001 s
2	100 x 100 = 10^2 = 10 000	0,01
8	10^8 = 100 000 000	100 s (1 min 40 s)
12	10^{12} = 1 000 000 000 000	1 000 000 s (11 jours env.)

* Les nombres de la 3e colonne sont obtenus en divisant ceux de la 2e colonne par 1 000 000.

Chiffrage d'un texte

texte stocké sous forme de nombre ↓ texte en clair ↓

Offset	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	
00000000	4C 65 20 63 69 65 6C 20 65 73 74 20 62 6C 65 75	Le ciel est bleu



le texte n'est plus lisible

Offset	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	
00000000	50 4B 03 04 33 00 01 00 63 00 33 6E 65 55 00 00	lHuBRWdw8ze2DUFb-jOEHKsWf3G2lXyuqJ-tiN/7Ds+4o=
00000016	00 00 2C 00 00 00 10 00 00 00 15 00 0B 00 65 78	
00000032	65 6D 70 6C 65 2D 63 68 69 66 66 72 61 67 65 2E	
00000048	74 78 74 01 99 07 00 02 00 41 45 03 00 00 B9 D3	
00000064	C4 FC 95 BOSF 43 F8 4F 5B B4 F5 F8 3D A5 4B CF	
00000096	E3 69 D7 02 B4 D9 F7 8F SF OD50 4B 01 02 3F 00	
00000112	33 00 01 00 63 00 33 6E 65 55 00 00 00 00 20 00	
00000128	00 00 10 00 00 00 15 00 2F 00 00 00 00 00 00 00	
0000144	20 00 00 00 00 00 00 00 65 70 ES 6D 70 EC 6S 20	
00000160	63 68 69 66 66 72 61 67 65 2E 74 78 74 0A 00 20	
00000176	00 00 00 00 00 01 00 18 00 BI CF F3 OF 15 F1 D8	
00000192	01 BA B1 08 28 15 F1 D8 01 37 02 0A CA 14 F1 D8	
00000208	01 01 99 07 00 02 00 41 45 03 00 00 50 48 05 06	
00000224	00 00 00 01 00 01 00 72 00 00 00 62 00 00 00 00	
00000240	00 00	

Retour

Exemple de hameçonnage

Lequel de ces messages est frauduleux ? Argumente ta réponse.

MESSAGE 1

Bonjour Utilisateur PayPal,

Dans le cadre de nos mesures de securite,

nous controlons regulierement les activites en cours dans le systeme PayPal. Au cours d'une recente verification, nous avons releve un probleme sur votre compte PayPal.

En etudiant votre compte, nous nous sommes rendu compte que nous avions besoin d'informations supplementaires pour vous fournir un service securise...

Cliquez ici pour activer votre compte

Lien sous « Cliquez ici ... » :
http://user-confirmation.com/acc/login.php

MESSAGE 2

Bonjour Madame Durand,

Afin de fournir un service de qualité, nos mesures de sécurité évoluent.

Des mises à jour de vos données personnelles sont nécessaires.

Pour cela, connectez-vous au service « Mon profil » dans votre espace personnel sur www.paypal.com.

Paypal vous remercie de votre confiance.

NB : Vous avez perdu vos identifiants ? **Cliquez ici** pour obtenir l'envoi d'un nouveau mot de passe.

Lien sous « Cliquez ici » :
https://www.paypal.com/cm/cshelp/article/jai-oubli%C3%A9-mon-mot-de-passe-comment-le-r%C3%A9initialiser%C2%A0-help143

MA RÉPONSE :

Retour

CORRIGÉ

Exemple de hameçonnage

Lequel de ces messages est frauduleux ? Argumente ta réponse.

MESSAGE 1

Bonjour Utilisateur PayPal,

Dans le cadre de nos mesures de securite,

nous controlons regulierement les activites en cours dans le systeme PayPal. Au cours d'une recente verification, nous avons releve un probleme sur votre compte PayPal.

En etudiant votre compte, nous nous sommes rendu compte que nous avions besoin d'informations supplementaires pour vous fournir un service securise...

Cliquez ici pour activer votre compte

Lien sous « Cliquez ici ... » :

http://user-confirmation.com/acc/login.php

MESSAGE 2

Bonjour Madame Durand,

Afin de fournir un service de qualité, nos mesures de sécurité évoluent.

Des mises à jour de vos données personnelles sont nécessaires.

Pour cela, connectez-vous au service « Mon profil » dans votre espace personnel sur www.paypal.com.

Paypal vous remercie de votre confiance.

NB : Vous avez perdu vos identifiants ? **Cliquez ici** pour obtenir l'envoi d'un nouveau mot de passe.

Lien sous « Cliquez ici » :

https://www.paypal.com/cm/cshelp/article/jai-oubli%C3%A9-mon-mot-de-passe-comment-le-r%C3%A9initialiser%C2%A0-help143

MA RÉPONSE :

Le message 1 est frauduleux pour plusieurs raisons.

- Son adressage n'est pas nominatif.
- Il comporte 16 erreurs d'orthographes dont 15 d'accent et une qui met une majuscule au mot utilisateur. Le message 2 n'en a pas.
- Il contient une maladresse d'expression : « Bonjour Utilisateur paypal ». Cet adressage n'est pas commun.
- Le message donne beaucoup d'explications futiles, pour convaincre.
- Un organisme sérieux propose toujours à l'internaute de se rendre sur le site officiel.
- Il ne compte pas de référence à Paypal, alors que le second en possède une.

Glossaire et conseils

Authentification par mot de passe :

L'utilisateur saisit ses identifiants (nom et mot de passe), et valide éventuellement un CAPTCHA.

Double authentification :

En plus de la saisie des identifiants, un message est envoyé par courrier électronique ou SMS.
Différentes méthodes d'authentification (surtout présentes sur les appareils mobiles, smartphones et tablettes) :

- mot de passe ;
- modèle de chemin (ou « motif »).
- biométrie avec reconnaissance :
  - de l'empreinte digitale d'un doigt ou scan de la main ;
  - d'une partie de l'œil comme la rétine ou l'iris ;
  - du visage (reconnaissance faciale) ;
  - de la voix (reconnaissance vocale).

Pour choisir un mot de passe :

- ne pas utiliser de dates, de prénoms ou de diminutifs, ou encore un mot de la langue du pays ou en anglais ;
- utiliser un mot de passe d'au moins 8 caractères ;
- cas particulier de l'utilisation d'une phrase : elle peut contenir des mots courants, sa solidité vient surtout de sa longueur (au moins 20 caractères). Difficile à décrypter tout en étant facile à retenir ;
- pour chaque accès à protéger, créer des mots de passe différents ;
- n'écrire le mot de passe nulle part. S'il y a plusieurs mots de passe à mémoriser, utiliser un logiciel coffre-fort avec un mot de passe général.

Pour se prémunir du hameçonnage :

- ne cliquer sur aucun lien, ne pas ouvrir les pièces jointes ;
- vérifier que le message mentionne votre nom ;
- vérifier que l'expéditeur soit sérieux. Si c'est une personne, être sûr de la reconnaître. S'il s'agit d'une organisation, vérifier sur Internet qu'elle existe et que les informations fournies dans le mail sont correctes ;
- le message doit être rédigé en bon français ;
- ne communiquer aucune information personnelle.