Introduction à la protection des données

Mandat	• Comparer les paramètres par défaut des différents réseaux sociaux • Thématiser les problèmes liés à la protection des données (en se basant éventuellement sur le dossier d'information, notamment sur le chapitre 1 «Qu'est-ce que la protection des données?») • Identifier les difficultés à venir résultant d'un manque de précaution • Feuille supplémentaire: «Voici ce que je divulgue sur ma personne!» A l'aide de cette feuille de travail, les élèves rapides peuvent réfléchir aux données qu'ils communiqueraient, et à qui ils les communiqueraient. La discussion qui en ressort peut se faire à deux, en groupe ou avec toute la classe.
Objectif	• Les élèves réfléchissent à ce qu'ils publient (ou souhaitent publier) sur les réseaux sociaux, et à la mesure dans laquelle les paramètres personnels le leur permettent. • Les élèves peuvent estimer les risques d'un transfert et d'un enregistrement de données non crypté.
Lien avec le programme scolaire	• MI.2.3n: «Les élèves peuvent estimer les risques d'un transfert et d'un enregistrement de données non crypté.»
Matériel	• Fiche «Discussion – données sensibles» • Captures d'écran «Paramètres de confidentialité» • Feuille de travail «Tableau»
Forme de travail	Travail individuel/à deux/avec toute la classe
Temps imparti	60 minutes

Informations complémentaires:

- La distribution de captures d'écran des paramètres de confidentialité de différents réseaux sociaux permet aux élèves de comparer et d'évaluer les différentes possibilités de réglage. Nous recommandons de le faire, car de nombreux jeunes se penchent (trop) peu sur la question des paramètres, et ne peuvent donc donner que des informations lacunaires sur leurs propres paramètres. Si l'on ne règle pas soi-même les paramètres par défaut, les services en ligne et les applications divulguent plus d'informations que nécessaire pour la fonction souhaitée (accès au carnet d'adresses, aux données de l'emplacement, par exemple).
- Pour expliquer les termes utilisés, le dossier «Protection des données» de la série de leçons peut être utilisé (par exemple réseau social, nuage).
- **Préposé fédéral à la protection des données et à la transparence (PFPDT)**
  Observations concernant les sites de réseautage social
  https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/Internet_und_Computer/services-en-ligne/medias-sociaux/observations-concernant-les-sites-de-reseautage-social.html

Ton compte est-il sûr?

Discussion
Compare avec ton voisin ou ta voisine de table si et comment les paramètres de confidentialité de vos réseaux sociaux diffèrent. Pour ce faire, utilisez les captures d'écran de la page suivante.

Exemples: Instagram, Google+, Snapchat, Facebook, kik, etc.

- Constatez-vous des **différences**?
  (Vie privée, sécurité, invitations à devenir amis, communications, etc.)
- Discutez également de ce qui change lorsque vous **modifiez les paramètres de votre profil.**
- Certains réglages sont-ils **absolument** nécessaires?
- Qu'est-ce qui ne **peut pas être modifié?**

➔ Notez vos constatations ci-dessous:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Le savais-tu?

Si les services de réseautage social sont le plus souvent gratuits, ils ne sont en rien des organisations caritatives. C'est «donnant-donnant»: ils offrent des prestations aux utilisateurs en échange de leurs données personnelles.

www.jeunesetmedias.ch
Indications et conseils pertinents sur les réseaux sociaux et les paramètres de sécurité recommandés.

Source d'images: Wepushbuttons
https://wepushbuttons.com.au/wp-content/uploads/2013/04/social-media-list.jpg

Exemple 1: paramètres de confidentialité Facebook (avril 2018)

Paramètres et outils de confidentialité

Votre activité	Qui peut voir vos futures publications ?	Amis	Modifier
	Examinez toutes les publications et tous les contenus dans lesquels vous êtes identifié(e)		Utiliser l'historique personnel
	Limiter l'audience des publications que vous avez ouvertes aux amis de vos amis ou au public ?		Limiter l'audience des anciennes publications
Comment les autres peuvent vous trouver et vous contacter	Qui peut vous envoyer des invitations à devenir amis ?	Tout le monde	Modifier
	Qui peut voir votre liste d'amis ?	Public	Modifier
	Qui peut vous trouver à l'aide de l'adresse e-mail que vous avez fournie ?	Amis	Modifier
	Qui peut vous trouver à l'aide du numéro de téléphone que vous avez fourni ?	Tout le monde	Modifier
	Voulez-vous que les moteurs de recherche en dehors de Facebook affichent votre profil ?	Oui	Modifier

Exemple 2: paramètres de confidentialité Twitter (avril 2018)

Confidentialité et sécurité

Confidentialité

Confidentialité
☐ Protégez vos Tweets
Si cette option est sélectionnée, seules les personnes que vous approuvez recevront vos Tweets. Vos prochains Tweets ne seront pas disponibles publiquement. Les Tweets que vous avez publiés précédemment peuvent toujours être visibles par tous à certains endroits. En savoir plus

Localisation
☐ Tweeter avec une localisation
Si cette option est sélectionnée, vous pouvez ajouter des informations de localisation à vos Tweets, comme votre ville ou votre localisation précise, depuis le Web et via des applications tierces. Ce paramètre n'affecte pas Twitter pour iOS ou Android. En savoir plus

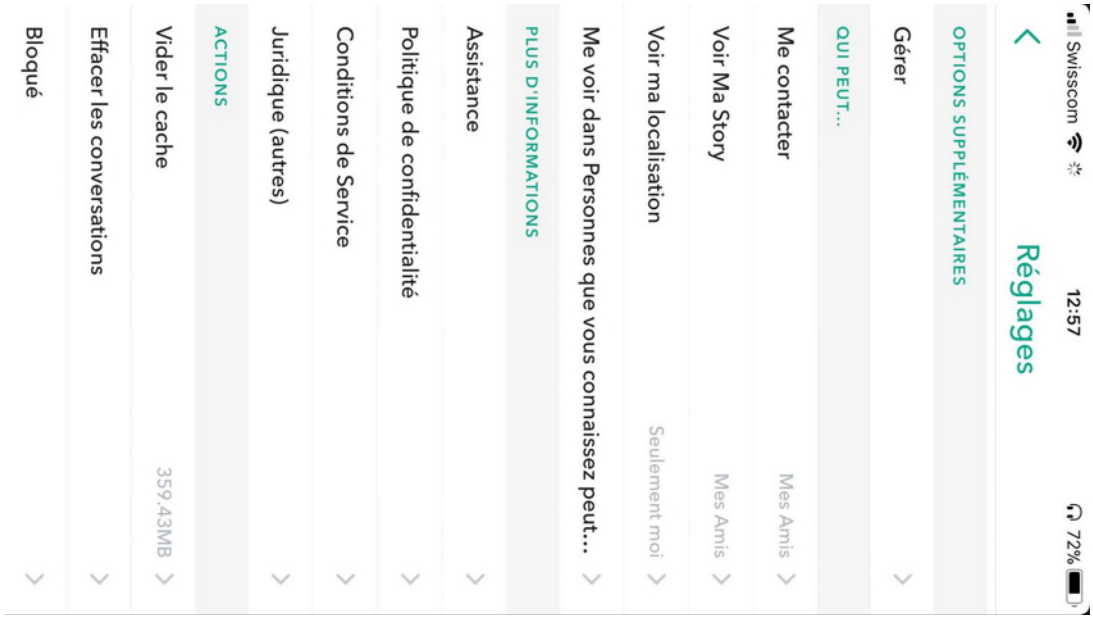
Supprimer les informations de localisation
Ceci supprimera les étiquettes de localisation que vous avez ajoutées à vos Tweets. Ceci peut prendre jusqu'à 30 minutes.

Identification de photo
◉ Autoriser tout le monde à vous identifier sur des photos
○ Autoriser uniquement les personnes que vous suivez à vous identifier sur des photos
◉ N'autoriser personne à vous identifier sur des photos

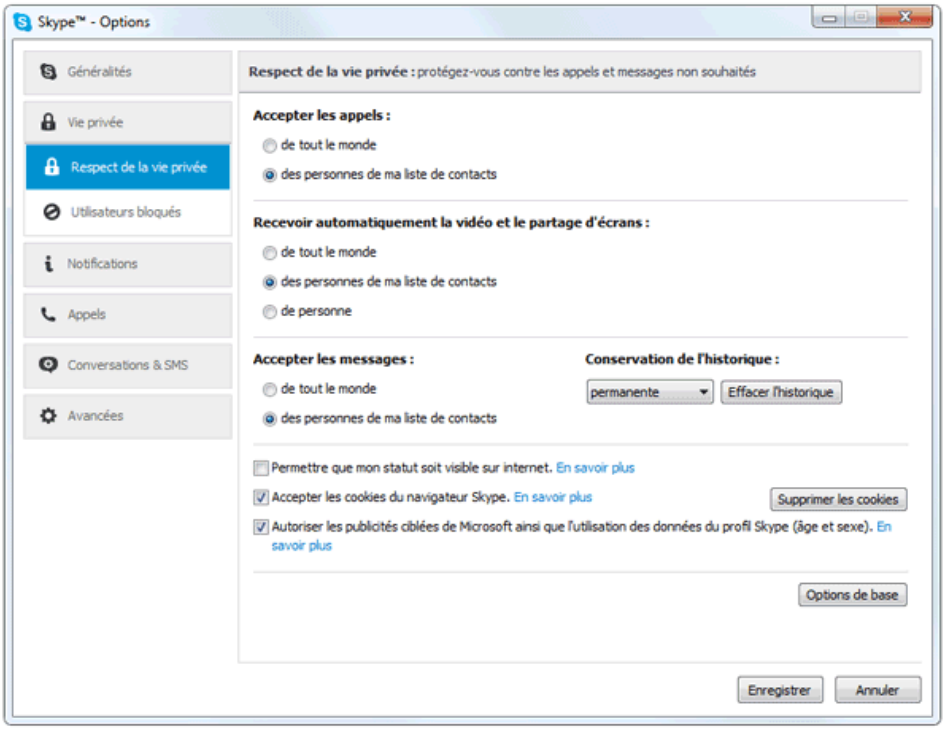
Détectabilité
☐ Permettre de me trouver grâce à mon adresse email
☐ Permettre de me trouver grâce à mon numéro de téléphone
Ce paramètre prendra effet une fois que vous aurez ajouté un numéro de téléphone. Ajouter maintenant
En savoir plus sur la façon dont ces données sont utilisées pour vous mettre en lien avec d'autres personnes

Carnet d'adresses
Gérer vos contacts
Contacts que vous avez téléchargés sur Twitter à partir de votre carnet d'adresses.

Exemple 3: paramètres de confidentialité Snapchat (avril 2018)



Exemple 4: paramètres de confidentialité Skype (avril 2018)



Lorsque les données tombent entre de mauvaises mains…

Exercice
Sélectionne une des situations suivantes et réfléchis à ce qui pourrait ensuite se passer.
Note en quelques mots un développement possible.

1. Une élève envoie des photos privées à un chat collectif. Ces photos la montrent lors d'une sortie, faisant la fête et consommant alcool et tabac.
2. Stéphane modifie la photo de son profil. Sur la photo, il pose dans le vestiaire du centre de fitness avec, en arrière-plan, un jeune homme en train de se changer.
3. Léa et son ami aiment échanger des photos par chat. Sur certaines photos, ils sont dévêtus. Quelque temps plus tard, ils se séparent en mauvais termes.
4. Michaël enregistre les données d'accès de à ses comptes de réseaux sociaux, de son compte en ligne et de son compte e-mail sur un nuage. Le site des exploitants du nuage ne se trouve cependant pas en Suisse et n'est donc pas soumis à la législation suisse sur la protection des données.
5. Michelle prend subrepticement des photos de ses camarades de classe et de ses professeurs. Elle les télécharge ensuite sur Instagram.
6. Philippe reçoit une invitation à devenir amis de la part d'une personne qu'il ne connaît pas sur Instagram. Il accepte, bien qu'il ne sache pas qui se cache derrière le profil.
7. Corinne reçoit un SMS de la part d'un numéro inconnu, lui demandant de lui communiquer ses données bancaires afin de les contrôler. L'expéditeur indiqué en fin de message est «Votre banque».
8. Francesco a un nouveau téléphone mobile. Il transfert les contenus de son ancien téléphone mobile vers le nouveau, mais oublie de définir un mot de passe. Le lendemain, il oublie son téléphone mobile dans le bus.

Suite…

……

……

……

……

……

Peux-tu imaginer d'autres exemples dans lesquels les données personnelles tombent entre de mauvaises mains et les problèmes pouvant en découler?

……

……

……

Voici ce que je divulgue sur ma personne!

Exercice
Dans le tableau ci-dessous, coche les informations que tu transmettrais à des groupes de personnes, ainsi que ces groupes.
Mets un (+) pour «Oui», un (–) pou «Non» et un (?), si tu n'es pas sûr.

	Famille	Collègues	Chef, enseignant	Abonné sur Instagram	Inconnus dans la rue	Inconnus sur les forums de chat
Age, sexe						
Groupe sanguin						
Indication sur les frères et sœurs, membres de la famille						
Salaire, emploi						
Photos de mon ami/de mon amie et moi						
Contacts commerciaux						
Liste de contacts de mon téléphone mobile						
Mon numéro de téléphone mobile						
Mon adresse e-mail						
Mon domicile						
Le code d'accès à mon téléphone mobile ou à mon ordinateur portable						
Une photo de mon visage						
Une photo de mon corps (habillé)						
Une photo de mon corps nu						
Le solde de mon compte						

	Famille	Collègues	Chef, enseignant	Abonné sur Instagram	Inconnus dans la rue	Inconnus sur les forums de chat
Des informations sur ma routine quotidienne						
Des informations personnelles apprises par une amie/un ami.						
Le mot de passe de mon compte sur un réseau social (par exemple Instagram, Facebook)						
Mon orientation sexuelle						

Compare ensuite tes réponses avec celles de tes camarades de classe.

Où sont les différences?
Où êtes-vous d'accord?
Quelles sont les données que je divulgue sur un réseau social?

Autres informations sur le sujet

Ouvrez l'œil: *Fausse identité sur un forum de chat (police municipale de Zurich)*
https://www.ouvrezloeil.ch/fr/harcelement

PFPDT: *Transfert de données de WhatsApp à Facebook*
https://www.edoeb.admin.ch/edoeb/fr/home/actualites/aktuell_news/transmission-de-donnees-de-whatsapp-a-facebook.html

Solutions possibles

Feuille de travail «Ton compte est-il sûr?»

➔ **Solutions individuelles des élèves**

Il est indispensable de souligner le fait que les paramètres de confidentialité requièrent une modification active. Sur Instagram, par exemple, le profil est par défaut accessible à tous. Si l'utilisateur souhaite être uniquement accessible pour ses amis («followers»), il doit lui-même modifier les paramètres de confidentialité.
Voir également (en allemand uniquement):
http://praxistipps.chip.de/privatsphaere-fuer-instagram-einstellen-so-klappts_12050

Feuille de travail «Lorsque les données tombent entre de mauvaises mains…»

Suites possibles et sujets de discussion:

Situation 1 *Les photos téléchargées sur un chat de groupe peuvent en principe être transférées à n'importe qui, voire être publiées sur Internet. Cela peut par exemple entraîner des problèmes avec les parents, les entreprises formatrices, etc.*

Situation 2 *Selon les paramètres de confidentialité, la photo du profil de Stéphane est visible pour les autres utilisateurs. Etant donné que Stéphane a photographié une autre personne sans son consentement exprès et qu'il a publié cette photo, les conséquences peuvent non seulement être d'ordre civil, mais aussi pénal. Et ce notamment, parce que la personne a été photographiée alors qu'elle se changeait.*

Situation 3 *Après leur séparation, ni Léa ni son ancien petit-ami ne peuvent contrôler l'utilisation des photos qu'ils se sont envoyées. D'abord, les photos peuvent être transmises et publiées, ce que la personne photographiée ne souhaite sans doute pas. Ensuite, la transmission et la publication de photos sans le consentement exprès de la personne photographiée constituent une infraction à la loi sur la protection des données et violent la vie privée de la personne concernée.*

Situation 4 *Etant donné que Michaël a enregistré ses données sur un nuage étranger, il ne peut pas être certain que ces données sont sauvegardées selon les normes suisses. Comme il s'agit de données confidentielles et de mots de passe, Michaël pourrait subir d'importants dommages en cas d'accès à ses données par des tiers non autorisés.*

Situation 5 *Michelle prend des photos sans autorisation des personnes photographiées pour les publier. Son comportement peut entraîner une responsabilité civile.*

Situation 6 *Il est déconseillé d'accepter les demandes d'ajout à la liste d'amis provenant d'inconnus, car il n'est pas possible d'être certain que cette personne n'a pas d'intentions illicites. A part soi-même, il est possible de mettre d'autres personnes dans des situations délicates ou dangereuses. Philippe doit être conscient du fait que cette personne pourra à l'avenir voir, utiliser, modifier ou publier tous les contenus qu'il partagera avec ses «amis».*

Situation 7 *Etant donné que les banques ne demandent jamais de données d'accès par SMS ou par e-mail, il faut supposer qu'une personne non habilitée souhaite obtenir les données bancaires de Corinne. Si Corinne les transmet, elle peut encourir un dommage financier. Il ne faut donc jamais ouvrir les documents joints ni cliquer sur les liens contenus dans ce type d'e-mails.*

Situation 8 *Etant donné que Francesco n'a pas codé son téléphone mobile, toute personne le trouvant aura accès à toutes les données, applications et contenus de son téléphone mobile. Des contenus privés et sensibles (photos, vidéos, messages, etc.) pourraient donc être interceptés, et les comptes de Francesco être utilisés pour filtrer ses contacts et contacter des personnes sous un faux nom.*

Pour plus d'informations sur les conséquences pénales en matière de protection des données, veuillez vous reporter aux sections «Images et droits d'image (2.7)»; «Dangers concrets et conséquences juridiques (2.4)» et «Smartphones (2.5)» du dossier d'information «Protection des données» lié à cette série de leçons.

Feuille supplémentaire «Voici ce que je divulgue sur ma personne!»

➔ *Solutions individuelles des élèves*