Club Informatique Gennois

Atelier – Les réseaux sociaux

Sommaire

- **Les différents réseaux sociaux**
- **Quels sont les dangers ?**
- **La sécurité**

Les différents réseaux sociaux

- **1 – Facebook (Meta), le réseau social aux 2,9 milliards d'utilisateurs actifs**

  - Avec ses **3 milliards d'utilisateurs actifs mensuels à travers le monde**, Facebook est sans nul doute le réseau social le plus populaire que le web ait connu actuellement.
  - En France, le réseau social rassemble chaque mois plus de 35 millions d'utilisateurs.
  - L'Inde compte le plus d'utilisateurs Facebook dans le monde (314,6 millions).

- **2 – YouTube, le média social dédié au partage et au visionnage de vidéos**

  - YouTube, propriété de Google, est le réseau social numéro 1 dans le partage et le visionnage de vidéos.
  - Le contenu proposé par YouTube fédère une communauté de plus de 2,5 milliards de personnes dans le monde, dont 41,4 millions en France.
  - Depuis quelques mois, la plateforme est proposée sous deux versions, une version gratuite accessible par le grand public, et une version payante, où les publicités sont supprimées.

Les différents réseaux sociaux

- **3 – WhatsApp, le réseau social dédié aux conversations**

  - Racheté par Facebook, WhatsApp est une application mobile gratuite permettant de passer des appels et d'envoyer des messages gratuitement lorsque l'on dispose d'une connexion internet, depuis et vers n'importe quel pays du monde.
  - Avec ses 2 milliards d'utilisateurs actifs dans le monde, WhatsApp est même devenue la plateforme la plus utilisée au quotidien, avec un taux d'ouverture quotidienne de 83,3 %.

- **4 – Instagram, le réseau social qui monte en flèche**

  - Instagram est un réseau social permettant le partage de photos, carrousel d'images et vidéos.
  - Le réseau social lancé en 2010 s'est fait connaître notamment grâce à ses filtres et ses options de retouche de photos qui permettent à n'importe qui de rendre ses photos plus attractives avant leur partage.
  - 2 milliards d'utilisateurs
  - En 2024, Instagram est considéré comme le réseau social préféré de la population dans le monde (16,5 %).

Les différents réseaux sociaux

- **5 – TikTok, les courtes vidéos en musique**

  - Lancée en 2016, TikTok est une application mobile permettant à ses utilisateurs de prendre de courtes vidéos et d'y associer une musique, des enregistrements de films/sketchs ou des sons.
  - L'application permet, tout comme Snapchat et Instagram, d'ajouter des filtres et effets sur les vidéos.
  - En 2020, l'application revendiquait déjà plus de 800 millions d'utilisateurs actifs mensuels.
  - En 2024, ce sont plus d'1,6 milliard d'utilisateurs actifs que recense la plateforme, ce qui la positionne parmi les réseaux sociaux qui connaissent le plus de croissance actuellement

Les différents réseaux sociaux

Classement	Réseau Social	Entreprise	Pays	Création	Utilisateurs actifs mensuels
1.	Facebook	Meta	Etats-Unis	2004	3 milliards
2.	YouTube	Alphabet	Etats-Unis	2005	2,5 milliards
3.	WhatsApp	Meta	Etats-Unis	2009	2 milliards
4.	Instagram	Meta	Etats-Unis	2010	2 milliards
5.	TikTok	Bytedance	Chine	2016	1,6 milliard
6.	WeChat	Tencent	Chine	2011	1,3 milliard
7.	Messenger	Meta	Etats-Unis	2011	1 milliard
8.	Telegram	Telegram	Emirats Arabes Unis	2013	800 millions
9.	Douyin	Bytedance	Chine	2016	752 millions
10.	Snapchat	Snap	Etats-Unis	2011	750 millions
11.	Kuaishou	Kuaishou	Chine	2011	685 millions
12.	X (Twitter)	X Corp	Etats-Unis	2006	620 millions
13.	Weibo	Sina	Chine	2009	605 millions
14.	QQ	Tencent	Chine	1999	560 millions
15.	Pinterest	Pinterest	Etats-Unis	2009	480 millions

Quels sont les dangers ?

1 - **ATTEINTE À LA VIE PRIVÉE :**

- Prenons l'exemple de WhatsApp:

- Rappelons-le, ce réseau social utilisé aujourd'hui par plus de 2 milliards de personnes a décidé la modification de ses conditions générales d'utilisation en janvier 2021.

Dans ces nouvelles conditions, il est question de partager vos données stockées sur l'application avec vos autres comptes sur les réseaux sociaux (Facebook, Instagram…).

Cette décision, motivée par la volonté de Facebook de créer un socle de communication commun entre toutes ses plateformes (Facebook, WhatsApp et Instagram), a été fortement critiquée.

Elle se donne le droit d'utiliser vos informations personnelles sans votre consentement.

Cela a permis notamment à d'autres plateformes plus « sécurisées » et pourtant moins bien connues, comme Telegram ou Signal, de glaner de nouvelles parts de marché.

Quels sont les dangers ?

2 - USURPATION D'IDENTITÉ :

- Vous ne devriez pas être surpris de trouver sur les réseaux sociaux des profils qui usurpent votre identité.

Le vol d'identité est, en effet, l'un des plus grands dangers de ces plateformes sociales. Bien que certaines d'entre elles, comme Facebook, aient rendu un peu plus sévère le processus de création d'un compte et d'authentification pour y accéder (authentification à deux facteurs), ce phénomène continue de se répandre.

- Sur certains réseaux, comme Twitter, il est encore possible de créer un profil fictif et de l'utiliser pour diffuser de fausses informations ou inciter à la haine.

Grâce à un « faux » compte, il est même possible de harceler ou d'envoyer des logiciels malveillants à d'autres personnes.

- Selon une étude du cabinet américain Javelin Strategy, les personnes actives sur les réseaux sociaux encourent un risque 30 % supérieur de se voir usurper leur identité sur le Web à ceux qui ne les utilisent pas.

Cette même enquête précise que ce pourcentage est de 46 % chez les personnes utilisant particulièrement Facebook, Instagram et Snapchat.

Une autre enquête menée par Privacy Affairs a révélé qu'un compte Facebook piraté se vend sur le Dark Web au prix de 65 $. Ce montant est de 45 dollars pour un compte Instagram et de 35 $ pour un compte Twitter. Vu son importance, un compte Gmail hacké est vendu quant à lui au prix de 76 $.

Quels sont les dangers ?

4 - CYBERINTIMIDATION ET CHANTAGE :

- Les réseaux sociaux sont un lieu courant pour les cyber-harceleurs. Profitant de la fragilité mentale de certaines personnes, ils n’hésitent pas à leur envoyer des messages dans le seul but de les intimider ou pire encore, les faire chanter.
- Le problème ici est que les plateformes sociales n’ont que très peu moyens de contrôles, pouvant filtrer les messages déplacés ou à caractères haineux. Il s’agit d’un danger récurrent dont les enfants et adolescents sont les premières victimes. Parfois, cela donne lieu à des événements tragiques.
- Selon le dernier rapport de l’association e-enfance.org, ce phénomène touche particulièrement les plus jeunes. 10 % d’entre eux disent avoir déjà subi du cyberharcèlement, tandis que 21 % affirment connaître d’autres enfants qui ont été harcelés sur le Web. Mais, le pourcentage le plus choquant est celui de l’impunité, puisque dans 56 % des cas les auteurs du harcèlement ne sont pas sanctionnés.

Quels sont les dangers ?

3 - INGÉNIERIE SOCIALE :

- Les réseaux sociaux sont un terrain fertile pour les pirates informatiques. Pour eux, ces plateformes sont le moyen idéal de faire ce que l'on appelle du « social engineering ».

- Le social engineering (ou ingénierie sociale) est une technique qui consiste tout simplement à entrer en contact avec un individu, dans le but de lui soutirer des informations sensibles ou de pirater ses données personnelles.

- Malheureusement, les réseaux sociaux facilitent grandement la mise en place de ce type d'attaque. Par exemple, il suffit qu'un hacker vous envoie un lien contenant un virus par messagerie privée et que vous cliquiez dessus pour que vos données soient volées.

- Ce lien prend généralement la forme d'un formulaire Web qu'il faut remplir et qui vous promet de gagner un cadeau, une réduction dans un magasin… Bien que très vieille, cette technique d'hameçonnage constitue toujours une des armes principales sur laquelle reposent les hackers pour pirater des comptes sur les réseaux sociaux.

La sécurité

1 - PROTÉGEZ L’ACCÈS À VOTRE COMPTE :

Vos comptes de réseaux sociaux contiennent des informations personnelles sensibles (identité, adresse postale ou de messagerie, numéro de téléphone, date de naissance, etc.), qui peuvent être convoitées par les cybercriminels.

Pour vous assurer que personne ne puisse utiliser votre compte à votre insu ou usurper votre identité, protégez bien l’accès à votre compte en utilisant des mots de passe différents et suffisamment robustes.

Si le service le propose, activez également la double authentification.

La sécurité

2 - VÉRIFIEZ VOS PARAMÈTRES DE CONFIDENTIALITÉ :

Par défaut, les paramètres de visibilité de vos informations personnelles (numéro de téléphone, adresse email…) et de vos publications sont souvent très ouverts.

Vos données peuvent ainsi être partagées à tous les abonnés du réseau social.

Il est généralement possible de restreindre cette visibilité en réglant la configuration de votre compte, afin de garder la maîtrise de ce que les autres utilisateurs voient de vos informations et de vos activités.

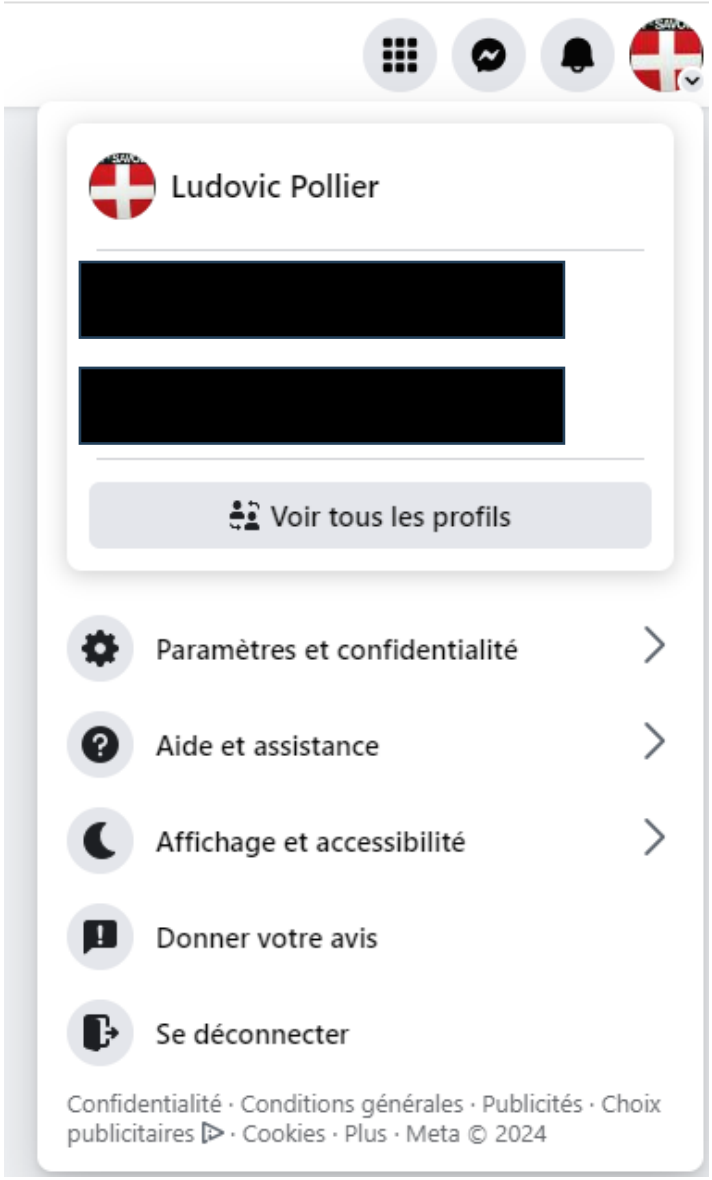
Vérifiez régulièrement ces paramètres de confidentialité qui peuvent être modifiés sans que vous ne le sachiez

La sécurité

Penons l’exemple de Facebook.

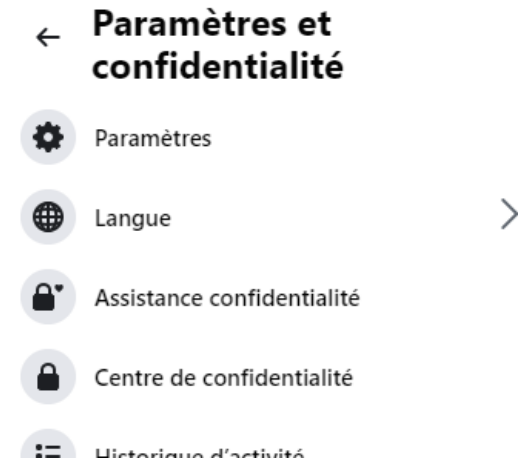
- Pour aller voir les paramètres de confidentialités, il faut cliquer sur l’icone de votre compte en haut à droite

- Cliquer ensuite sur « Paramètres et confidentialité »



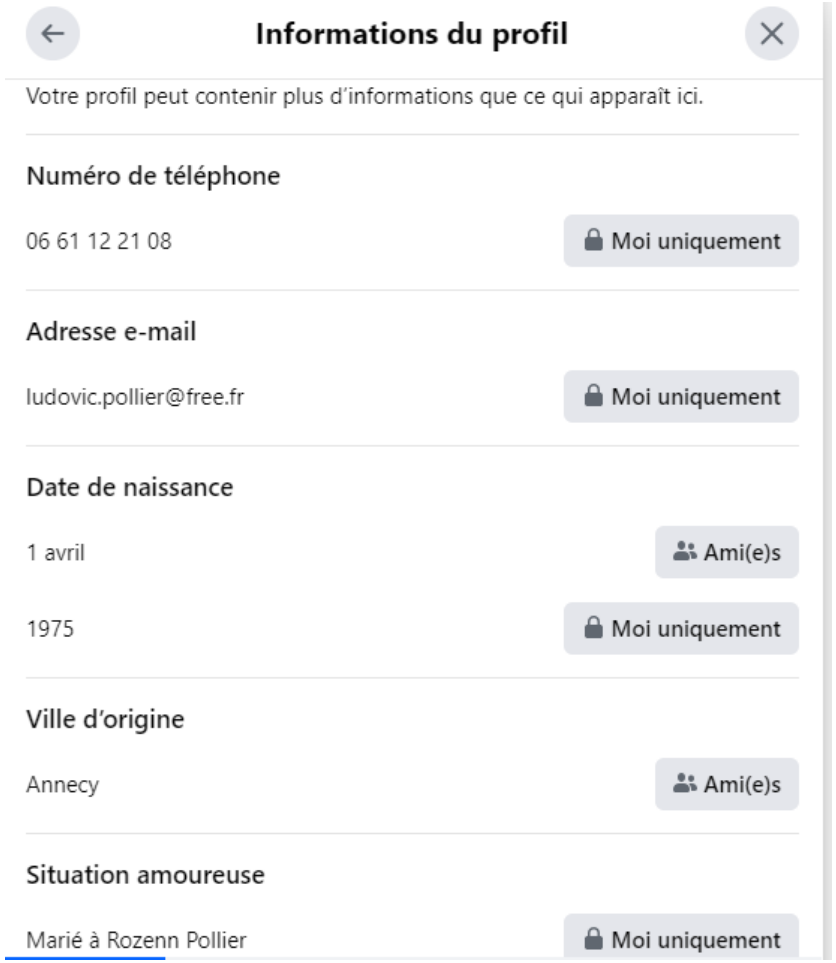
La sécurité

- Cliquer ensuite sur « Assistance confidentialité »



La sécurité

Ensuite, il vous suffit de cliquer sur une des vignettes et de vérifier les infos



La sécurité

3 - MAÎTRISEZ VOS PUBLICATIONS :

Les réseaux sociaux permettent de communiquer auprès d'une grande audience que vous ne pourrez jamais complètement maîtriser.

Même dans un cercle que l'on pense restreint, vos publications peuvent vous échapper et être rediffusées ou interprétées au-delà de ce que vous envisagiez.

Ne diffusez pas d'informations personnelles ou sensibles qui pourraient être utilisées pour vous nuire.

Faites également preuve de discernement lorsque vous évoquez votre travail car cela pourrait vous porter préjudice ainsi qu'à votre entreprise.

Enfin, respectez évidemment la loi.

La sécurité

4 - FAITES ATTENTION À QUI VOUS PARLEZ :

Les cybercriminels utilisent notamment les réseaux sociaux pour commettre des escroqueries et voler des informations personnelles ou professionnelles.

Soyez vigilants, car à leur insu, vos « amis » ou contacts peuvent également vous envoyer ou partager des contenus malveillants, surtout s'ils se sont fait pirater leur compte sans le savoir.

Quelques conseils supplémentaires :

- n'envoyez jamais d'argent à quelqu'un sans avoir vérifié son identité au préalable,
- n'envoyez jamais de photos ou vidéos intimes à des contacts virtuels qui pourraient en profiter pour vous faire chanter
- méfiez-vous des jeux concours, des gains inattendus, ou des « super affaires », qui peuvent cacher des escroqueries

La sécurité

5 - CONTRÔLEZ LES APPLICATIONS TIERCES :

Certaines applications proposent d'interagir avec votre compte de réseau social. Il peut s'agir de jeux, de quiz, de programmes alternatifs pour gérer votre compte.

Ces applications demandent des autorisations qu'il faut examiner avec attention car une fois données, ces applications peuvent avoir accès à vos informations personnelles, vos contacts, vos publications, vos messages privés…

Ne les installez que depuis les sites ou magasins d'applications officiels, sinon vous risquez de donner l'accès à votre compte à un programme infecté par un virus.

Si l'application vous semble trop intrusive dans les autorisations qu'elle demande, ne l'installez pas.

Enfin, pensez à désinstaller ces applications ou en révoquer les droits si vous ne vous en servez plus.

La sécurité

6 - ÉVITEZ LES ORDINATEURS ET LES RÉSEAUX WIFI PUBLICS :

Utiliser un ordinateur en libre accès ou un réseau WiFi public est risqué car ils peuvent être piégés ou contrôlés par un cybercriminel.

Lorsque vous vous connectez à votre compte de réseau social par ce moyen, vous pouvez vous faire voler votre mot de passe et donc vous faire pirater votre compte.

Évitez dans la mesure du possible de renseigner des in- formations sensibles ou personnelles sur un matériel ou un réseau qui n’est pas le vôtre.

Si vous y êtes contraint malgré tout, pensez à bien vous déconnecter de votre compte après utilisation pour empêcher que quelqu’un puisse y accéder après vous.

La sécurité

7 - VÉRIFIEZ RÉGULIÈREMENT LES CONNEXIONS À VOTRE COMPTE :

La plupart des réseaux sociaux offrent des fonctionnalités qui vous permettent de voir les connexions ou sessions actives sur votre compte depuis les différents appareils que vous utilisez pour y accéder.

Consultez régulièrement ces informations.

Si vous détectez une session ou une connexion inconnue ou que vous n’utilisez plus, déconnectez-la.

Au moindre doute, considérez qu’il peut s’agir d’un piratage et changez immédiatement votre mot de passe (voir conseil n°1).

La sécurité

Lieu de votre connexion

15 mai 2024

[redacted] était connecté sur PC Windows.
Création 19 janv. 2024, 00:19 Mise à jour 15 mai 2024, 14:53 Adresse IP 82.64.120.94 Navigateur Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36 Avast/123.0.0.0 Cookie G6Cp**********
14:53

[redacted] était connecté sur Xiaomi Redmi Note 12.
Création 27 mai 2023, 12:22 Mise à jour 15 mai 2024, 11:25 Adresse IP 37.169.83.225 Navigateur Dalvik/2.1.0 (Linux; U; Android 14; 22111317G Build/UKQ1.230917.001) [FBAN/Orca-Android;FBAV/455.0.0.40.107;FBPN/com.facebook.orca;FBLC/fr_FR;FBBV/591231677;FBCR/Free;FBMF/Xiaomi;FBBD/Redmi;FBDV/22111317G;FBSV/14;FBCA/arm64-v8a:null;FBDM/{density=2.75,width=1080,height=2176};FB_FW/1;] Cookie 8dlx**********
11:25

[redacted] était connecté sur Xiaomi Redmi Note 12.
Création 27 mai 2023, 12:22 Mise à jour 15 mai 2024, 09:31 Adresse IP 37.169.144.112 Navigateur [FBAN/FB4A;FBAV/461.0.0.47.85;FBBV/591544958;FBDM/{density=2.75,width=1080,height=2176};FBLC/fr_FR;FBRV/0;FBCR/Free;FBMF/Xiaomi;FBBD/Redmi;FBPN/com.facebook.katana;FBDV/22111317G;FBSV/14;FBOP/1;FBCA/arm64-v8a:;] Cookie V508**********
09:31

2 janvier 2024

[redacted] était connecté sur PC Windows.
Création 17 mai 2023, 22:08 Mise à jour 2 janv. 2024, 19:41 Adresse IP 82.64.120.94 Navigateur Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36 Avast/120.0.0.0 Cookie hFri**********
19:41

La sécurité

8 - FAITES PREUVE DE DISCERNEMENT AVEC LES INFORMATIONS PUBLIÉES :

Les réseaux sociaux sont de formidables et rapides outils d'information, mais n'importe qui peut aussi y publier n'importe quelle information, sans aucune vérification.

Certaines informations peuvent donc être partiellement ou totalement fausses, parfois délibérément.

Avec la puissance des réseaux sociaux, ces fausses informations (appelées « fake news » en anglais) peuvent avoir de graves conséquences sur les personnes qui en sont victimes.

Aussi, avant de considérer ou relayer une information, efforcez-vous d'en vérifier la véracité.

La sécurité

9 - UTILISEZ EN CONSCIENCE L'AUTHENTIFICATION AVEC VOTRE COMPTE DE RÉSEAU SOCIAL SUR D'AUTRES SITES :

Pour s'y connecter, certains sites Internet vous proposent d'utiliser votre compte de réseau social.

Cette fonctionnalité peut sembler pratique car elle évite de créer un compte et un mot de passe supplémentaires, mais cela signifie que vous allez communiquer au réseau social des informations sur ce que vous faites sur le site concerné, et à l'inverse que vous allez peut-être donner au site des droits d'accès sur votre compte de réseau social.

De plus, si votre compte de réseau social était un jour piraté, le cybercriminel pourrait automatiquement accéder à tous ces sites en usurpant votre identité.

Aussi, avant d'utiliser cette fonctionnalité, ayez bien conscience des risques et vérifiez attentivement les autorisations que vous délivrez.

La sécurité

10 - SUPPRIMEZ VOTRE COMPTE SI VOUS NE L’UTILISEZ PLUS :

Pour éviter que vos informations ne soient récupérées par des tiers ou que votre compte ne soit utilisé à votre insu, notamment pour usurper votre identité, supprimez-le si vous ne l’utilisez plus.

La sécurité

Que faire en cas de problème ?

- Demander la suppression d'une publication gênante ou compromettante sur les réseaux sociaux : les conseils de la CNIL
- Être conseillé face à situation de cyberharcèlement : contacter le 3018, ligne d'écoute nationale anonyme et confidentielle destinée aux internautes confrontés à des problèmes dans leurs usages numériques.
- Signaler un contenu illicite sur les réseaux sociaux : Internet-signalement.gouv.fr