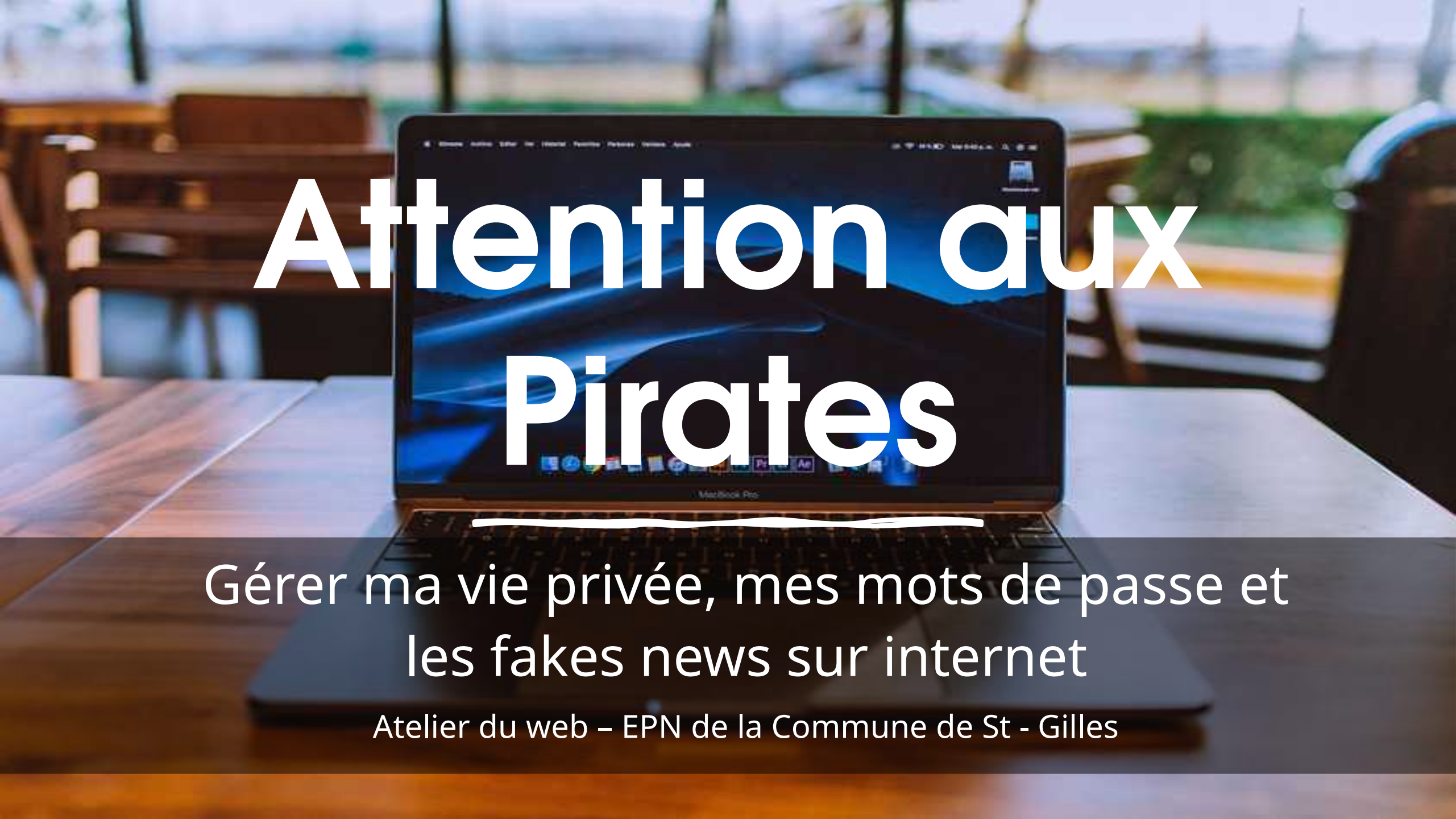


Attention aux Pirates

Gérer ma vie privée, mes mots de passe et les fakes news sur internet

Atelier du web – EPN de la Commune de St - Gilles

Introduction

- Depuis l’avènement des réseaux dit sociaux, un nombre incalculable d’informations qui relèvent du privé sont exposées et échangées entre les utilisateurs.
- Dans certains cas cela peut se révéler un danger et emmener à des dérives.
- Que faire du coup pour éviter les nombreux pièges.

Quels sont les risques ?

1. Usurpation d’identité (Phishing)
2. Vol de compte (mot de passe faible)
3. Harcèlement en ligne
4. Collecte de données et marketing ciblé
5. Fake News

1. Usurpation d’identité

L’usurpation d’identité, qu’est-ce que c’est ?

Une usurpation d’identité est une utilisation de données personnelles propres à vous identifier sans votre accord.

Une fois volées, ces informations peuvent servir aux usurpateurs pour nuire à votre réputation, réaliser des opérations financières ou commettre des actes répréhensibles en votre nom.

Comment s’en protéger ?

Faire attention à contenus que l’on poste sur les différents plateformes (Facebook, tik tok…), donner les moins de détails sur votre vie privé

Installez des logiciels antivirus et antimalware fiables.

Veillez à mettre régulièrement à jour votre système d’exploitation et vos autres logiciels

Faites attention lorsque vous cliquez. (lien et pièces jointes reçu dans son mail)

Veillez à protéger votre smartphone.

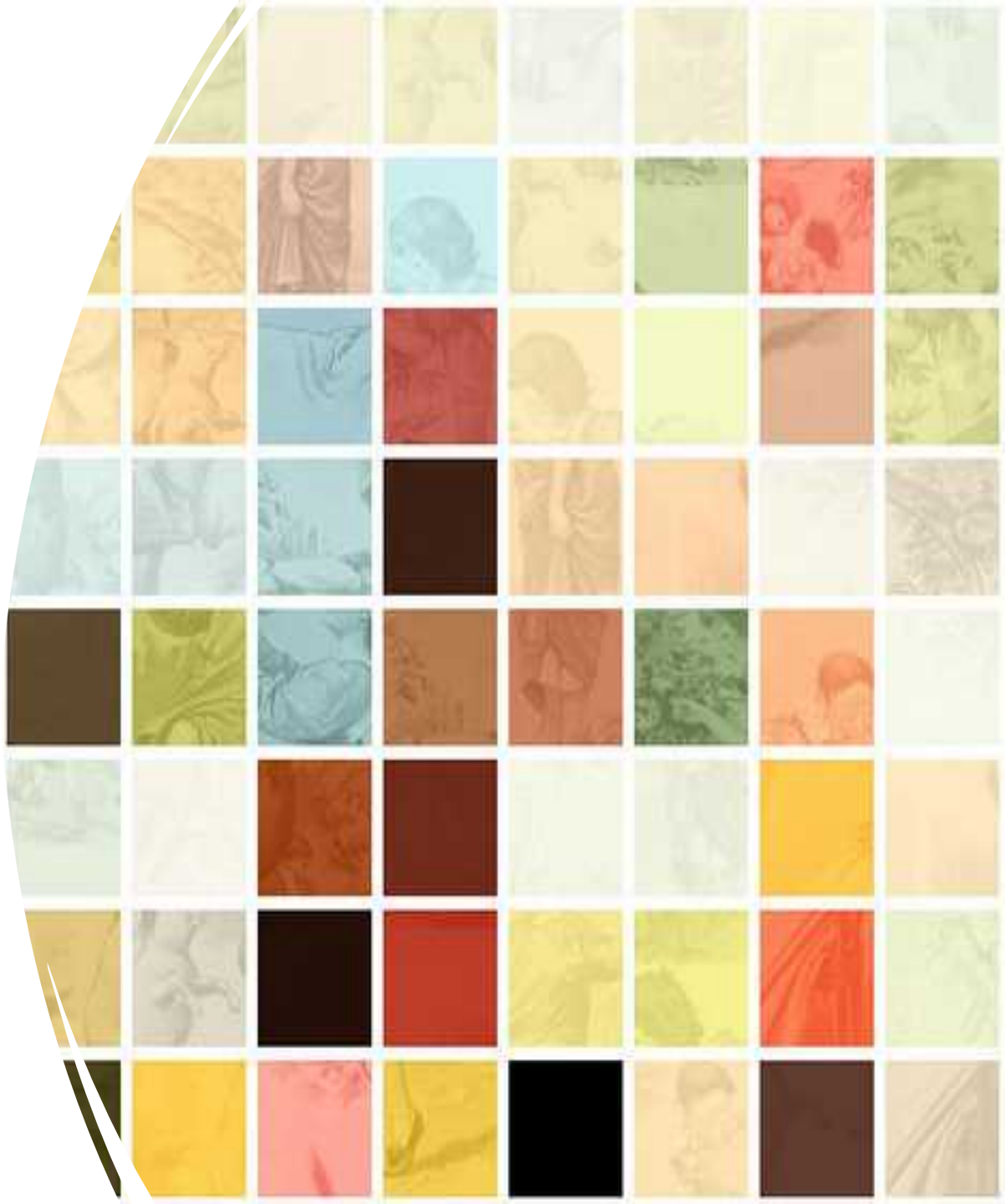
Utilisez des mots de passe forts pour sécuriser vos appareils, votre accès à Internet et vos comptes.

Protégez votre vie privée et votre sécurité en ligne en utilisant autant que possible l’authentification à deux facteurs

2. Mes mots de passes

La liste des mots de passe à ne surtout pas choisir

- password
- 123456
- 123456789
- guest
- qwerty
- 12345678



Comment créer un mot de passe sécurisé ?

12 caractères ou 3 mots.

Des chiffres, des lettres, des majuscules et des caractères spéciaux.

Un mot de passe unique par compte.

Ajouter un numéro de téléphone de récupération. (Si possible)

Pas d'infos perso ni de mots courants.

Soignez tout particulièrement la sécurité de vos comptes mail.

3. Harcèlement en ligne

Le cyberharcèlement consiste en des **agissements malveillants répétés**, dans un cadre public ou restreint, qui peuvent prendre **différentes formes** : *intimidations, insultes, menaces, rumeurs, publication de photos ou vidéos compromettantes, etc.*

Le but recherché est clairement la dégradation psychologique de la victime.

Ce phénomène est criant particulièrement chez les adolescents qui sont encore en quête d'identité.

Les 13-15 ans sont les plus touchés par le cyberharcèlement.

Comment (se) prémunir (les enfants) du cyberharcèlement ?

Réfléchir avant d'envoyer un message ou de publier une photo de soi ou de ses amis.

Ne renseignez votre profil qu'avec le minimum d'informations nécessaires.

Maîtrisez vos cercles de connaissances, vos amis, sur les réseaux sociaux.

Faites attention à qui vous parlez

Gérez vos paramètres de confidentialité (Mettre ses compte en « privé »).

Parler de harcèlement, c'est commencer à agir.

Que faire en cas de cyberharcèlement ?

1. **Ne répondez pas** aux commentaires ou aux messages qui s'apparentent à du cyberharcèlement.
2. **Parlez-en à un tiers de confiance**. la famille (conjoint, parents, frères, sœurs, etc.), à un ami, ou encore, dans le cadre scolaire, à un adulte de l'école ou à un camarade de classe.
3. **Conservez les preuves**. Faites des captures d'écran, conservez les messages et les informations liées aux auteurs du cyberharcèlement, qui pourront vous servir pour signaler et caractériser cette situation, voire pour déposer plainte.
4. **Verrouillez au plus vite les comptes de réseaux sociaux**.
5. **Signalez les contenus ou les comportements illicites auprès des plateformes sur lesquelles ils sont présents afin de les faire supprimer.** :**Facebook**, **Twitter**, **LinkedIn**, **Instagram**, **Snapchat**, **TikTok**, **WhatsApp**, **YouTube**...;
6. **Demandez à ce que les contenus harcelants ne soient plus référencés par les moteurs de recherche et** demander un déréférencement. Faites une demande auprès de chaque moteur de recherche concerné : **Bing**, **Qwant**, **Google**, **Yahoo**, **autres**.
7. **Déposez plainte à la CERT (Cyber Emergency Response Team).** **www.cert.be**

4. Collecte de données et marketing ciblé

- Aujourd’hui nos données privées sont collectées de manières massive à des fins publicitaires.
- Une fausse gratuité !
- On utilise le terme Big Data car la quantité des données collectées est exponentielle.
- Ces données(data) sont donc une source non négligeable de revenues pour les publicitaires

Comment limiter cette collecte ?

Changez de navigateur web (Firefox)

Utilisez un gestionnaire de mots de passe (Bitwarden)

Changez de moteur de recherche (Startpage, Ecosia, duckduckgo…)

Modifiez votre DNS(open dns, cloudflare…)

Communiquez à l’aide de messageries chiffrées (Signal, Telegram…)

Utilisez une connexion VPN (Mullvad, ProtonVPN)

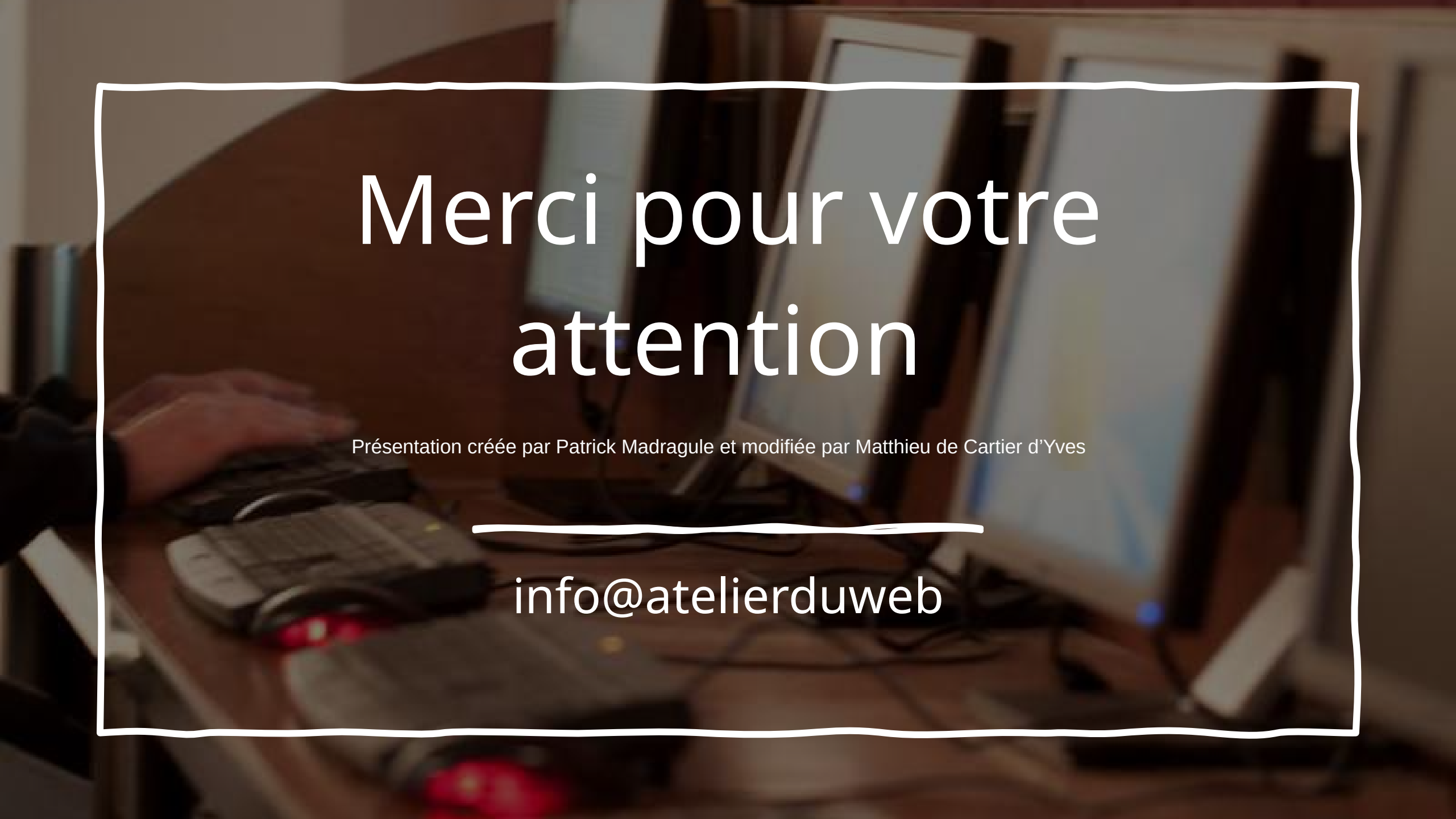
Utiliser un bloqueur de pub (ublock, adnauseaum….)

5. Fake News et esprit critique

- Vérifier la crédibilité des sources avant de partager une information.
- Apprenez à questionner les sources, à vérifier les faits et à effectuer des recherches supplémentaires
- **Faky**, l’outil anti-fake news

Conclusion : 5 conseils pour protéger ma vie privée sur les réseaux sociaux

1. J'ai conscience	que mes données personnelles ont de la valeur !
2. Je protège	ma vie privée en utilisant des pseudonymes et des Avatars.
3. Je verrouille	mon compte ! D'abord en le sécurisant avec un mot de passe fort et en activant les options complémentaires comme la « double authentification ».
4. J'anticipe	les conséquences de mes publications ! Internet est un lieu public où je peux laisser des traces.
5. Je vérifie	les informations auxquelles j'ai accès avant de les partager ou de cliquer dessus.



Merci pour votre attention

Présentation créée par Patrick Madragule et modifiée par Matthieu de Cartier d’Yves

info@atelierduweb