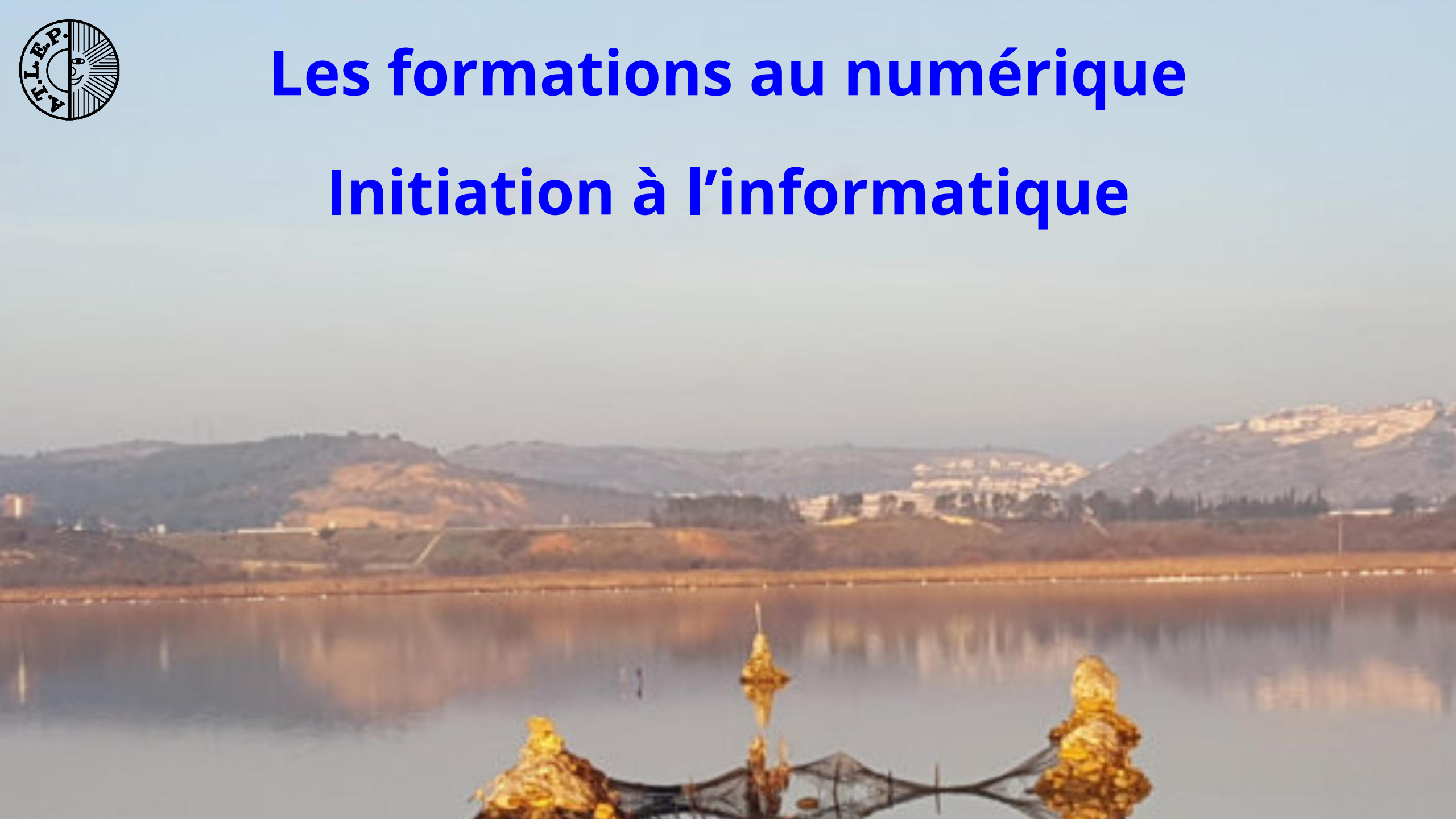
Les formations au numérique

Initiation à l'informatique



Naviguer sur Internet

Comment chercher une information

Comment choisir un résultat

La fenêtre de navigation

Télécharger une image

Se connecter aux « bons clics »

Comment organiser ses fichiers et ses dossiers ?

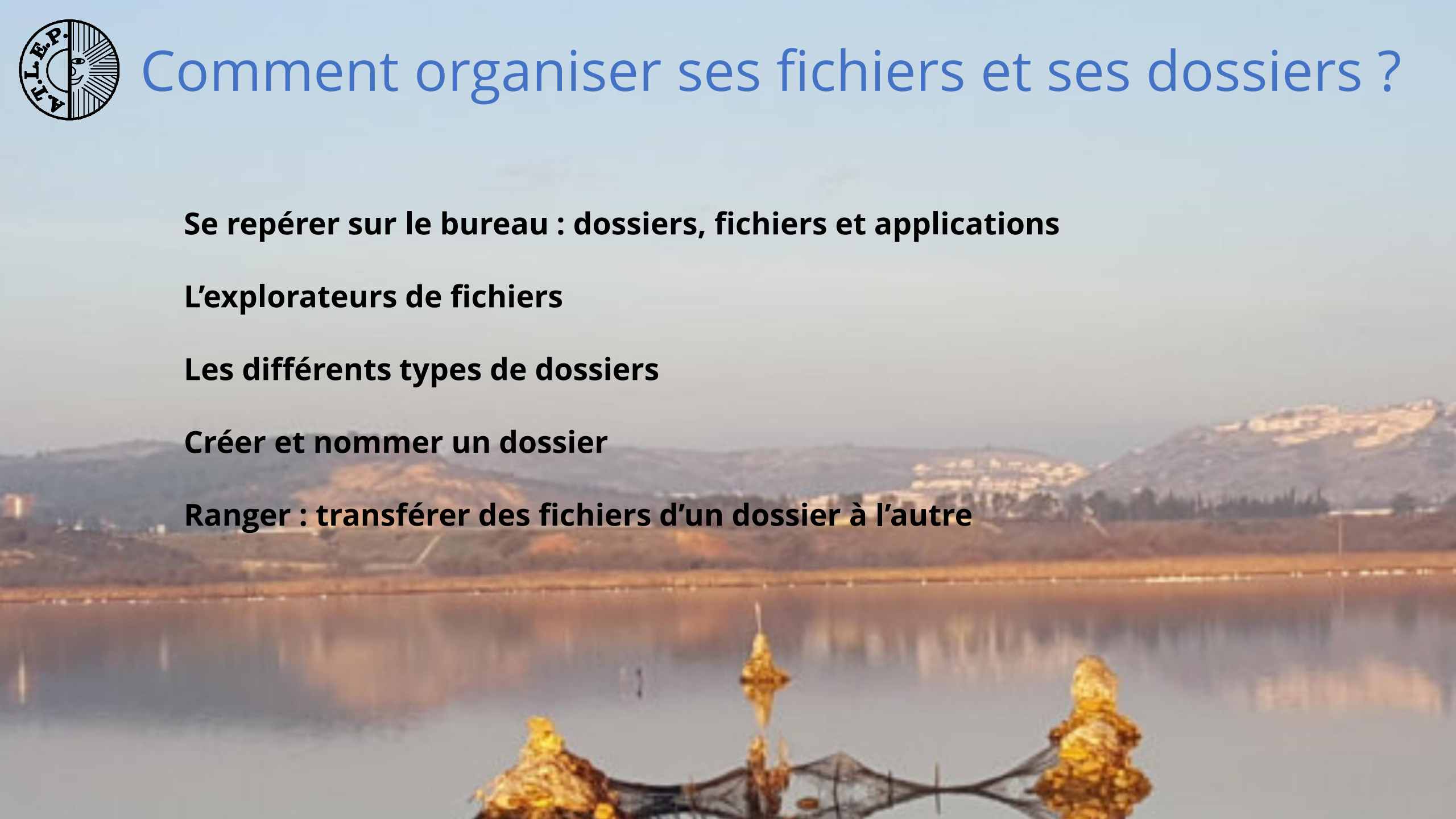
Se repérer sur le bureau : dossiers, fichiers et applications

L'explorateurs de fichiers

Les différents types de dossiers

Créer et nommer un dossier

Ranger : transférer des fichiers d'un dossier à l'autre



La messagerie mail?

La messagerie mail, a quoi ça sert

Les adresses mail

Les différents gestionnaires de messagerie

Envoyer et recevoir un mail

Recevoir et classer une piece jointe

Envoyer une piece jointe

La securité sur internet

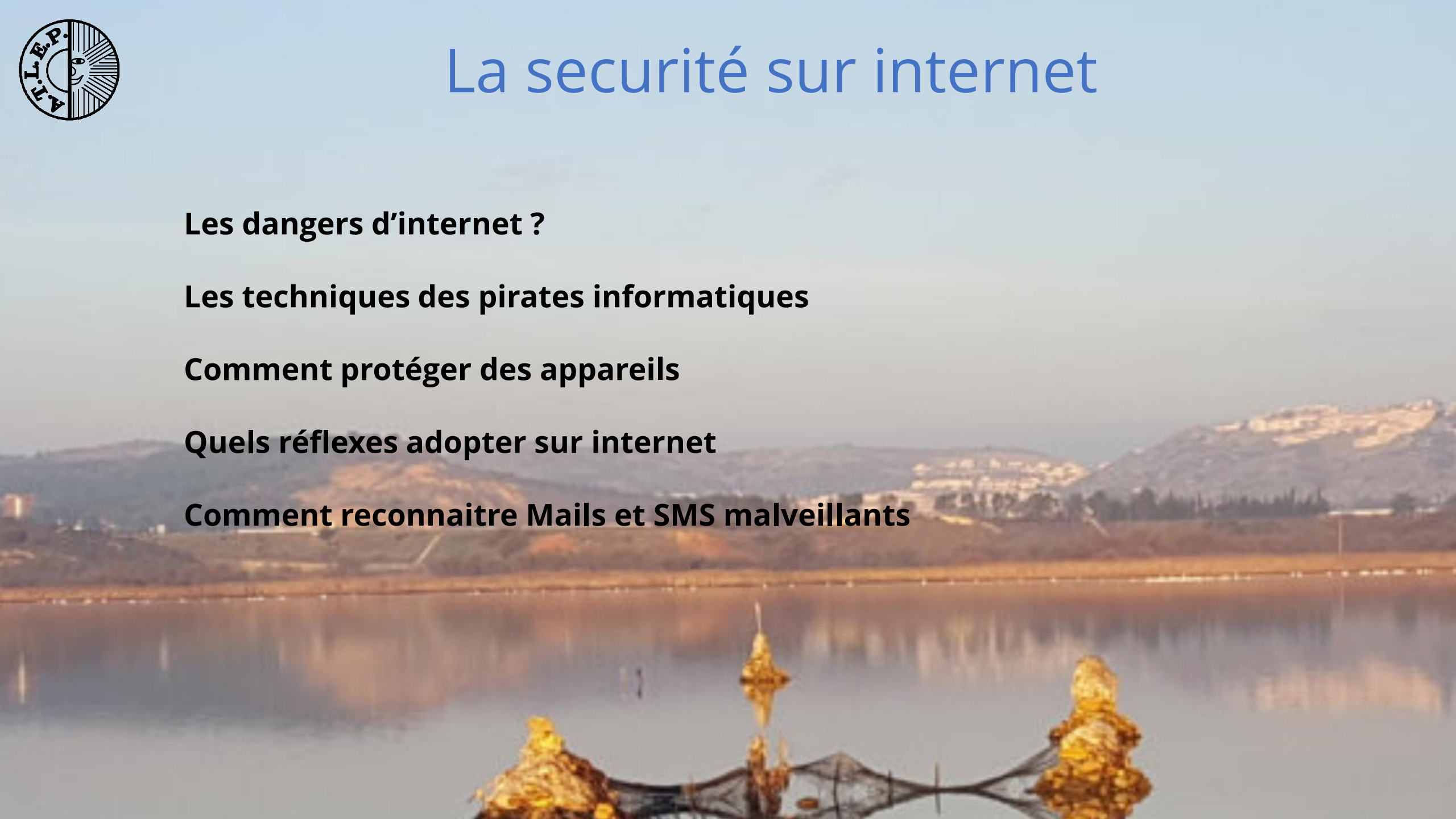
Les dangers d'internet ?

Les techniques des pirates informatiques

Comment protéger des appareils

Quels réflexes adopter sur internet

Comment reconnaitre Mails et SMS malveillants



Le piratage informatique

Le piratage informatique: c'est quoi le problème?

https://youtu.be/Lnpn-AZ9Qzo

Quel moyens utilisent les pirates informatique

Les moyens :

En cliquant ci-dessus lien vers les bons clics

L'absence d'antivirus

Si vous ne protégez pas votre ordinateur ou vos appareils mobiles (smartphones, tablettes ...), les pirates pourront l'infecter avec des

Les sites non sécurisés

Beaucoup de personnes naviguent sur des sites internet non sécurisés, et les pirates en profitent pour obtenir leurs données personnelles !

Réseau wifi non sécurisé

Si vous utilisez le réseau wifi public pour réaliser des transactions importantes (par exemple un paiement en

Les mails et les SMS

Très souvent, les pirates utilisent le mail ou le SMS : pour transférer un virus, pour envoyer une arnaque, pour vous inciter à cliquer sur un

Les fausses promesses

Pour toucher leurs victimes, il arrive que les pirates promettent des choses incroyables : un emploi de rêve, une grosse somme d'argent...

Les sentiments

Les pirates exploitent parfois les sentiments de leurs victimes : par exemple, en se faisant passer pour un ami qui a besoin d'argent.

Comment se protéger ?

Inutile de taper sur le clavier à toute vitesse et à quatre mains, ou de débrancher l'ordinateur ! L'attaque a lieu sur le réseau internet, elle se propagera même si vous éteignez l'ordinateur. Le meilleur moyen d'éviter les attaques informatiques est d'appliquer des règles simples de sécurité en ligne :

Accès
Video

- **Installer un antivirus**
- **Naviguer sur des sites fiables**
- Privilégier les **réseaux wifi sécurisés**
- Ne pas répondre aux **mails suspicieux**
- Protéger ses **données personnelles**, en ne les partageant pas
- Faire des **sauvegardes régulières** de vos fichiers personnels, par exemple sur un disque dur externe (**à privilégier**) ou un service de stockage en ligne

L’antivirus

L'antivirus est l'équivalent de la ceinture de sécurité en voiture.

A retenir

- La ceinture est **obligatoire** pour sécuriser ses déplacements en voiture. C'est pareil pour l'antivirus sur ses appareils informatiques.
- La ceinture n'est **pas suffisante** : elle ne permet pas d'éviter tous les accidents. Il faut aussi être prudent sur la route. Avec l'antivirus, c'est la même chose : il faut aussi être vigilant lorsqu'on navigue sur l'internet et repérer soi-même les dangers.
- Une seule ceinture de sécurité par passager. De même, il ne faut installer qu'**un seul** antivirus pour que celui-ci soit vraiment efficace.

avast

Avast est un antivirus gratuit et efficace

Windows 10

Windows 10 intégre un antivirus : Windows defendeur automatiquement installé sur les ordinateurs en W10

Paramétrer son navigateur internet

Paramétrer son navigateur pour quoi faire ?

Bien choisir et paramétrer votre navigateur est important car c'est votre porte d'entrée sur l'internet, selon la situation : ordinateur ou smartphone professionnel/personnel, partagé/individuel. **Vous devez :**

1. Effacer votre historique de navigation et données de formulaires
2. Supprimer vos cookies et vos mots de passe (notamment si l'appareil est partagé)
3. Vider le cache du navigateur

Limiter ses traces sur internet

Une navigation internet sécurisée

A retenir

1. Pour faire des transactions bancaires ou confidentielles, connectez-vous sur un **réseau wifi sécurisé**

2. Vérifiez toujours que le **site est sécurisé** : en vérifiant que l'adresse du site est correcte et que le "https" est bien présent.

3. Utilisez des **mots de passe** sécurisés

4. Si vous utilisez un ordinateur partagé avec d'autres personnes, **déconnectez-vous** de vos comptes personnels quand vous avez terminé.

Reconnaitre les Mails et SMS malveillants

1. Regardez l'**adresse mail** de l'expéditeur : est-elle fiable ? Si une entreprise ou une organisation vous envoie un mail finissant par gmail, outlook, laposte, etc, alors ce mail est suspect.

2. Repérez s'il y a des **fautes d'orthographe**

3. Regardez si le message est **personnalisé** : la plupart du temps, les messages envoyés par les pirates ne mentionnent ni votre nom ni votre prénom.

4. Si on vous demande des **informations personnelles ou de l'argent**, méfiez-vous

5. Si l'offre est **trop belle pour être vraie**, c'est peut-être une arnaque.