

# MAIRE # Faire face aux risques Cyber

Les menaces ?	Principe ?	Comment gérer...Se Protéger ?
 Défaçage	<ul style="list-style-type: none"> <li>→ <b>Attaque du code</b> informatique de la page et modification visuelle de celle-ci</li> <li>→ Atteinte à l'image</li> </ul>	<ul style="list-style-type: none"> <li>- Sensibilisation / formation des personnels</li> <li>- Mise à jour logiciels / antivirus</li> <li>- Ne pas cliquer sur pièce jointe ou lien de mails frauduleux</li> </ul>
 Rançongiciel	<ul style="list-style-type: none"> <li>→ Apparition d'une fenêtre indiquant le <b>blocage du système et cryptage des données.</b></li> <li>→ Victime invitée à <b>payer une rançon</b> pour recouvrer ses données.</li> </ul>	<ul style="list-style-type: none"> <li>- Je vérifie l'adresse mail du site</li> <li>- Je ne donne pas mes coordonnées bancaires</li> <li>- Sauvegardes régulières</li> </ul>
 Phishing	<ul style="list-style-type: none"> <li>→ Réception d'un mail contenant un <b>lien</b> ou une <b>pièce jointe</b> vous incitant à enregistrer vos identifiants personnels sur une page piratée</li> <li>→ Vol de vos identifiants</li> </ul>	<ul style="list-style-type: none"> <li>- Je n'insère pas de supports amovibles non vérifiés</li> <li>- Je rédige une charte informatique</li> </ul>
 Piratage	<ul style="list-style-type: none"> <li>→ <b>Intrusion dans le système</b> informatique</li> <li>→ vol, introduction de malwares, etc.</li> </ul>	<ul style="list-style-type: none"> <li>- Une personne s'occupe de la gestion du parc informatique</li> <li>- Je signale les faits et je dépose plainte à ma Gendarmerie</li> </ul>

## Vérifier mon IMMUNITÉ CYBER

**I** Inventaire complet

**M** Mots de passe

**M** Mises à jour & sauvegardes

**U** Utilisateurs sensibilisés

**N** Neutralisation des virus

**I** Informatique et libertés

**T** Télétravail en sécurité

**É** Évaluation

## Conséquences directes et indirectes d'un piratage...

- Pertes, vol, diffusions de **données sensibles**
- **Interruption d'activité** (perte connexion internet, système inexploitable, impossibilité de répondre aux usagers...)
- **Perte de crédibilité et atteinte à l'image** de la collectivité du Maire et de ses équipes
- Possible **absence de prise en charge** par les assurances
- **Coûts significatifs** liés au rétablissement de l'activité
- **Responsabilité** au titre du RGPD

## Les bons réflexes

### Protéger ses données

- Ne communiquez pas de données sensibles par mail ou SMS** (code CB, mot de passe...): aucun organisme ne vous les demandera
- Attention aux SMS et emails douteux:** ne cliquez pas sur les liens et ne répondez pas aux messages. Vérifiez l'adresse e-mail de l'émetteur
- Mettez à jour régulièrement vos appareils et vos logiciels.** Pensez aussi à faire des sauvegardes de vos données
- Activez l'authentification en deux étapes** sur vos comptes : vous recevrez un SMS à chaque connexion pour sécuriser davantage l'accès à votre compte
- Choisissez des mots de passe **sécurisés et différents** pour chaque site Internet
- Vérifiez que le site Internet est **bien sécurisé**, en regardant si l'URL commence bien par **https://** et un cadenas fermé

GENDARMERIE  
NOTRE ENGAGEMENT, VOTRE SÉCURITÉ