MAIRE # Faire face aux risques Cyber

Les menaces ?		Principe ?	Comment gérer...Se Protéger ?
	Défaçage	→ Attaque du code informatique de la page et modification visuelle de celle-ci → Atteinte à l'image	- Sensibilisation / formation des personnels - Mise à jour logiciels / antivirus - Ne pas cliquer sur pièce jointe ou lien de mails frauduleux - Je vérifie l'adresse mail du site - Je ne donne pas mes coordonnées bancaires - Sauvegardes régulières - Je n'insère pas de supports amovibles non vérifiés - Je rédige une charte informatique - Une personne s'occupe de la gestion du parc informatique - Je signale les faits et je dépose plainte à ma Gendarmerie
	Rançongiciel	→ Apparition d'une fenêtre indiquant le blocage du système et cryptage des données. → Victime invitée à payer une rançon pour recouvrer ses données.	
	Phishing	→ Réception d'un mail contenant un lien ou une pièce jointe vous incitant à enregistrer vos identifiants personnels sur une page piratée → Vol de vos identifiants	
	Piratage	→ Intrusion dans le système informatique → vol, introduction de malwares, etc.	

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