- Association Familiale du Malzieu-Ville
- Atelier informatique

[IN] Mémo participant - Sécurité numérique de base

Objectif : se protéger sur Internet contre les arnaques et le vol de données.

---

1. Créer un bon mot de passe

Les règles

- **12 caractères minimum**
- Mélanger : majuscules, minuscules, chiffres, symboles
- **Différent** pour tous les sites
- Ne jamais le partager

Technique : la phrase de passe

« J'adore les croissants ! » -> `J'@dore-les-CrOissants!`

---

2. Reconnaître une arnaque (hameçonnage/phishing)

Signes d'alerte

- Message **urgent** (« Votre compte sera fermé ! »)
- **Fautes** d'orthographe
- Adresse email **bizarre**
- Demande de **mot de passe** ou infos bancaires

Que faire ?

1. **Ne pas cliquer** sur les liens
2. **Ne pas répondre**
3. **Supprimer** l'email
4. En cas de doute, aller sur le site officiel directement

---

3. Protéger ses données personnelles

Ne jamais donner

- Mot de passe par email ou téléphone
- Numéro de carte bancaire par email
- Numéro de sécurité sociale
- Photo de sa carte d'identité

Scénarios à connaître

- **Banque appelle** : Raccrocher et appeler avec le numéro connu
- **Facebook demande ID** : Refuser et signaler le profil
- **SMS "CB utilisée"** : Ne pas appeler le numéro donné
- **Technicien à domicile** : Refuser de donner le mot de passe

---

4. Gérer ses applications

Permissions à vérifier

- **Caméra** : nécessaire pour cette app ?
- **Localisation** : autoriser uniquement lors de l'utilisation
- **Contacts** : vraiment utile ?
- **Photos** : accès limité si possible

Réflexes apps

- **Refuser** les permissions non nécessaires
- **Préférer** "uniquement lors de l'utilisation"
- **Supprimer** les apps trop gourmandes en données

---

5. Bonnes pratiques quotidiennes

Réflexes de sécurité

- **Email suspect** : Ne pas cliquer, supprimer
- **Wi-Fi public** : Éviter les opérations bancaires
- **Mises à jour** : Accepter rapidement les mises à jour de sécurité
- **Clé USB trouvée** : Ne jamais la brancher
- **Pop-up antivirus** : Fermer et ne rien télécharger

---

6. En cas de problème

Actions immédiates

- **Arnaque bancaire** : appeler sa banque immédiatement (3179)
- **Compte piraté** : changer le mot de passe
- **Vol de données** : signaler sur internet-signalement.gouv.fr

Contacts utiles

- **Cybermalveillance** : 0800 887 887 (gratuit)
- **Phishing** : signaler@phishing-initiative.fr
- **Signalement** : internet-signalement.gouv.fr

Gardez ce mémo précieusement, il vous servira tous les jours !