Check-list — 5 gestes pour mieux se protéger (Zone sécurité)

Salon des métiers du numérique 2026 — Association Hubmonster.io
Document public — sensibilisation ; ne remplace pas un **avis juridique** ni une **intervention d'urgence** (gendarmerie, banque, etc.).

Avant de commencer

- ☐ Je suis sur **mon** téléphone ou **mon** ordinateur (pas un PC public sans garantie).
- ☐ Je n'écris **jamais** mon mot de passe, mon code SMS ou mon RIB dans le **chat** d'un salon ou d'une visio.

---

1. Double authentification (2FA / MFA)

- ☐ J'ai activé la **double authentification** sur au moins **un** compte important (mail pro, messagerie, réseau social le plus sensible, espace bancaire si proposé).
- ☐ Je privilégie une **application d'authentification** ou une **clé de sécurité** plutôt que le SMS **quand c'est possible**.

Pourquoi : un mot de passe volé suffit rarement si la 2e étape est en place.

---

2. Mots de passe uniques + coffre-fort (gestionnaire)

- ☐ J'utilise un **mot de passe différent** pour les services importants (mail, banque, messagerie pro).
- ☐ J'ai installé ou j'utilise un **gestionnaire de mots de passe** reconnu (et un **mot de passe principal** fort pour le coffre).

Pourquoi : une fuite sur un site n'empêche pas la réutilisation ailleurs si tout est identique.

---

3. Sauvegardes

- ☐ Mes **photos / documents importants** existent **à au moins deux endroits** (ex. appareil + cloud ou disque externe chiffré).
- ☐ Je vérifie que je peux **ouvrir** une sauvegarde test (pas seulement « la copie existe »).

Pourquoi : ransomware, vol, casse — ce qui n'existe qu'une fois peut disparaître d'un coup.

---

4. Mises à jour (système, navigateur, applications)

- ☐ J'ai lancé les **mises à jour** en attente sur le **téléphone** ou le **PC** (ou planifié une fenêtre de maintenance courte).
- ☐ J'ai mis à jour le **navigateur** utilisé pour l'administration sensible.

*Pourquoi : les mises à jour corrigent souvent des **failles** déjà connues des attaquants.*

---

5. Signalement en cas d'arnaque ou d'abus

- ☐ En cas de **tentative** ou de **vol** en ligne : je signale sur **Cybermalveillance** (point d'entrée national) et je contacte **ma banque** si un paiement est en jeu.
- ☐ Je garde une **trace** (captures d'écran, e-mails) **sans** retourner jouer le jeu de l'arnaqueur.

Lien utile : cybermalveillance.gouv.fr

En une page — les 5 idées

#	Geste
1	**2FA** sur les comptes critiques
2	**Mots de passe uniques** + gestionnaire
3	**Sauvegardes** testées
4	**Mises à jour** faites
5	**Signalement** + traces si incident

Dernière mise à jour du contenu : document généré pour le salon 2026 — vérifier les liens officiels au moment de l'événement.