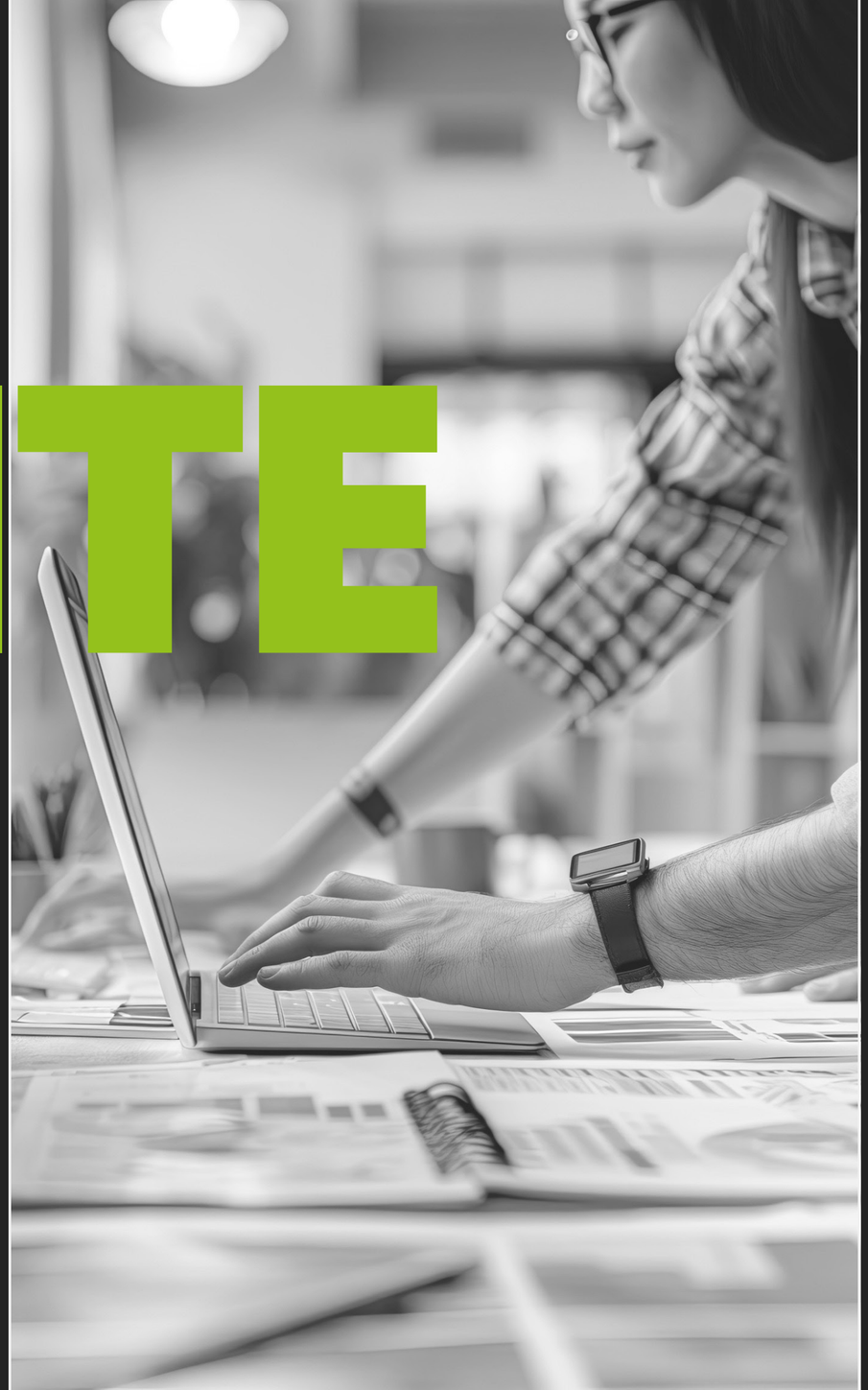
CYBER SECURITE



Protégez vos données et votre identité numérique avec ces **5 cyber réflexes essentiels** : mots de passe solides, mises à jour régulières, sauvegardes sécurisées, vigilance face aux arnaques et prudence sur les contenus en ligne.

1 CHOISIR DES MOTS DE PASSE SOLIDES ET DIFFÉRENTS POUR CHAQUE COMPTE

Un mot de passe c'est comme une clé propre à chaque porte, elle protège de l'intrusion. Si le mot de passe est volé, et qu'il est utilisé pour différents sites web ou applications, ils pourront tous être piratés !

- Utiliser des mots de passe suffisamment longs, complexes et différents pour chaque compte

- Les garder secrets (ne pas les communiquer) et privilégier un gestionnaire de mot de passe sécurisé pour les conserver

2 FAIRE LES MISES À JOUR DES APPAREILS ET DES LOGICIELS SANS TARDER

Les failles de sécurité des logiciels, applications et matériels sont comme des portes laissées ouvertes pour les pirates. Ils peuvent les utiliser pour accéder à nos données personnelles ou les voler.

- Activer les options de mises à jour automatiques chaque fois que c'est possible

- Faire les mises à jour des logiciels, applications et appareils, dès qu'elles sont proposées pour corriger leurs failles de sécurité.

3 CONSERVER EN LIEU SÛR UNE COPIE DES DONNÉES

Copier les données, c'est les sauvegarder pour éviter de les perdre en cas de piratage, de vol, de panne ou de casse des appareils.

- Penser à faire régulièrement des sauvegardes des données sur un autre support (clé USB, disque externe, cloud...) pour pouvoir les retrouver en cas de problèmes

4 SE MÉFIER
DES MESSAGES INATTENDUS ET/OU ALARMANTS

L'hameçonnage ou phishing, ce sont des messages (courriels, SMS, réseaux sociaux) ou appels d'escrocs qui se font passer pour un organisme familier (banque, administration...).

Ces arnaques visent à voler des informations personnelles et bancaires, faire télécharger un virus ou directement nous escroquer.

- Toujours se méfier et ne pas se précipiter pour répondre

- Vérifier toujours l'infirmation par soi-même, en se connectant à son compte sur le service concerné

5 ÉVITER LES CONTENUS NON OFFICIELS

Des virus qui peuvent pirater nos appareils ou nos comptes sont souvent présents dans les logiciels piratés, les sites de streaming illégaux...

- Ne pas télécharger des contenus illégaux ni des solutions non officielles

Pour pallier le point 5, il faut installer un antivirus, et en se conformant au point 2, il faut qu'il soit toujours à jour.

- Installer uniquement des applications depuis les sites ou magasins officiels des éditeurs