

# Brochure de Sécurité

## Module 231 | Favre-Bulle

Le but de cette brochure est de sensibiliser, aider, et prévenir les utilisateurs des risques.

Chaque risque a donc des mesures de sécurité, la brochure est là pour cela, pour vous indiquer quoi faire dans telle ou telle situation.

### Contenu :

- Protection physique du matériel
- Supports amovibles
- Webcam, assistants vocaux et autres objet connectés
- Mise à jour des logiciels
- Stratégie de sauvegarde de données
- Bonnes mesures



E-mail : [diego.besse@bluewin.ch](mailto:diego.besse@bluewin.ch)

## Protection physique du matériel

la protection physique du matériel est essentielle pour garantir la sécurité des biens matériels.

Les principaux risques sont :

- **Vol de matériel**
  - Donc potentiellement perte de données
- **Accès non autorisé**
  - Des individus non autorisés peuvent accéder aux locaux où le matériel est stocké
- **Dommages causés par accidents** ou par des **catastrophes naturelles**
  - Inondations par exemple.
    - Soit par accident (bouteille d'eau)
    - Soit par catastrophe naturelle due a la pluie par exemple.

### Que faire pour éviter cela au maximum ?

**Mise en place de systèmes d'alarmes ou d'installation de protection physique :**

Se protéger pour éviter qu'un individu accède a des armoires d'appareils électronique par exemple.

**Mise en place de code PIN sur les appareils électronique :**

Pour éviter que si une personne s'introduise dans une salle de rangement de matériels puisse accéder aux contenu.

**Toujours placer les appareils électronique dans des endroits stratégique et réfléchis :**

Pour éviter tout type de dégâts sur le matériel.

## Supports amovibles

Les supports amovibles sont des **supports de données**, qui, comme leur nom l'indique, peuvent être **transférés d'un ordinateur à un autre**.

Ce sont typiquement les disques optiques, comme **CD** ou **DVD**, mais aussi les **disques durs externes**, les **memory-sticks** ou autres..

### La prudence est requise avec les supports amovibles !

### Quels sont les risques ?

- Vecteur virus
- Fuite de données
- Perte – Destruction

### Les mesures à entreprendre :

#### Les mesures minimales sont :

- Désactiver l'exécution automatique.
- Lancer systématiquement une analyse antivirus.

#### Principales mesures et bonnes pratiques :

- Eviter les échanges et les prêts .
- Désactiver l'exécution automatique.
- Lancer systématiquement une analyse antivirus.
- Eviter le formatage « rapide ».
- Chiffrer les données.
- Stocker correctement (valise, étui, mise sous clé, armoire de sécurité, armoire antifeu, etc...)

## Webcam, assistants vocaux et autres objets connectés

Faire attention aux risques liés à l'utilisation abusive des supports tels que les caméras, la géolocalisation, les micros intégrés et d'autres technologies de suivi est essentielle dans un monde de plus en plus connecté.

Ces risques peuvent toucher la vie privée, la sécurité et la confidentialité des individus.

## Que faire pour éviter cela au maximum ?

### Mettez à jour vos appareils :

Assurez-vous que vos objets électroniques sont toujours dotés des dernières mises à jour de sécurité.

### Utilisez des mots de passe forts :

Protégez vos appareils avec des mots de passe forts et uniques. Évitez d'utiliser des mots de passe par défaut et utilisez plutôt une combinaison de lettres, de chiffres et de caractères spéciaux.

Vous pouvez également activer l'authentification à deux facteurs (2FA) si c'est possible.

### Réseau Wi-Fi sécurisé :

Assurez-vous que votre réseau Wi-Fi est sécurisé en utilisant un chiffrement fort (comme WPA3) et en changeant régulièrement le mot de passe de votre réseau.

### Mettez en place un suivi de sécurité :

Utilisez des outils de surveillance de sécurité pour détecter les activités suspectes sur vos appareils électroniques.

### Ne pas télécharger d'applications douteuses :

Évitez de télécharger des applications provenant de sources non fiables ou de sites Web douteux. Utilisez les boutiques d'applications officielles pour télécharger des applications.

### Cacher la webcam de ses appareils :

Pour éviter d'être surveillé et/ou que des informations privées et confidentielles soient vues, cachez votre webcam avec un scotch opaque par exemple.

## Mise à jour des logiciels (anti-virus, MS update, pare-feu, etc...)

L'analyse de risques liés aux mises à jour logicielles sont une pratique essentielle pour garantir la stabilité, la sécurité et la performance des systèmes informatiques.

### Principaux risques :

- Exploitation de vulnérabilités non corrigées.
- Attaques de logiciels malveillants.
- Interruption du service antivirus.
- Incompatibilité des mises à jour avec d'autres logiciels.



### Astuces :

- Mettre les mises à jour en semi automatique, ou pour par exemple recevoir des alertes quand des mises à jours sont disponibles.
- Vérifier souvent si une nouvelle mise à jour est disponible.
- Utiliser des outils de surveillance pour détecter toute anomalie durant les mises à jour et mettre en place des alertes en cas de problème.
- Effectuer des tests de compatibilité avec d'autres logiciels.
- Mettre en place des mécanismes de sauvegarde avant les mises à jour.

## Stratégie de sauvegarde des données

La mise en place d'une stratégie de sauvegarde des données est cruciale pour assurer la sécurité et la disponibilité des informations importantes pour une organisation.

Cependant, il existe plusieurs risques potentiels liés à cette stratégie.

### Perte de données lors de la sauvegarde :

- **Risque** : Les erreurs humaines, les pannes matérielles ou les problèmes de logiciel peuvent entraîner une perte de données pendant le processus de sauvegarde.
- **Mesures** : Utiliser des solutions de sauvegarde fiables, effectuer des tests réguliers de restauration pour s'assurer que les données peuvent être récupérées avec succès.

### Sécurité des données sauvegardées :

- **Risque** : Les données sauvegardées peuvent être exposées à des menaces de sécurité, y compris les attaques de ransomware, les accès non autorisés, etc.
- **Mesures** : Chiffrer les données sauvegardées, mettre en place des contrôles d'accès assez stricts, et utiliser des solutions de sécurité pour détecter et prévenir les attaques.

### Obsolescence technologique :

- **Risque** : Les technologies de sauvegarde peuvent devenir obsolètes, rendant difficile la récupération des données à l'avenir.
- **Mesures** : Mettre à jour régulièrement les solutions de sauvegarde pour rester en phase avec les avancées technologiques, planifier la migration vers de nouvelles technologies lorsque cela est nécessaire.

### Conformité légale et réglementaire :

- **Risque** : Non-respect des exigences légales et réglementaires en matière de sauvegarde des données, ce qui peut entraîner des sanctions et des poursuites.
- **Mesures** : Assurer la conformité avec les lois et réglementations en vigueur, mettre en place des politiques de rétention des données conformes.

## Mot de Passes :

Les principaux risques sont :

- Usurpation d'identité
- Utilisation frauduleuse
- Prise de contrôle
- Attaque par brute force



## Principales mesures :

- Verrouiller sa session quand nous nous absentons de notre poste de travail
- Ne pas utiliser le même mot de passe pour plusieurs utilisations différentes
- Utiliser une application de gestionnaire de mot de passe, coffre fort de mot de passe
- Ne pas laisser les mots de passes par défauts fournis de base, et en mettre de nouveau
- Activer l'authentification à deux facteurs est fortement recommandé
- Mettre un mot de passe avec des chiffres, des majuscules et des minuscules, des caractères spéciaux, et avec 12 caractères ou +

Les principales mesures ci-dessus sont recommandées pour éviter au maximum de se faire pirater nos mots de passes.



## BONNES MESURES

### Principaux risques

Sessions :

- Accès non autorisé sur notre session et du coup risques de voir des données confidentielles ou autres.
- Indiscrétion. Par exemple, quelqu'un pourrait voir des choses privées ou confidentielles.

Navigation internet :

- Risque de traçage (marketing ou malveillant)
- **Vol d'identité**, des cybercriminels peuvent tenter de voler votre identité en recueillant des informations personnelles, ce qui peut entraîner des conséquences graves telles que la fraude financière.
- Les attaques de phishing



### Bonnes mesures pour éviter cela

Sessions :

- Verrouiller sa session systématiquement lorsqu'on quitte son poste de travail.
- Activer le verrouillage automatique en cas d'inactivité au poste de travail (au bout de quelques temps inactif).

Navigation internet :

- Activer le verrouillage automatique en cas d'inactivité au poste de travail.

## BONNES MESURES



### Principaux risques

Messagerie :

- **Accès non autorisé sur notre session** et du coup risques de voir des données confidentielles ou autres.
- **Fuites de données**
  - Divulcation involontaire ou volontaire des données.
- Des individus malveillants pourraient accéder aux comptes de messagerie sans autorisation.

### Principales mesures :

- Authentification à deux facteurs
- Politiques de mot de passe robustes
- Surveillance des connexions suspectes.



# BONNES MESURES

## Principaux risques

- **Suspicion d'accès frauduleux**
  - Coûts (rançons, réparations, etc...)
  - Paralysie de l'activité

## Bonnes mesures pour éviter cela

- **PROCESSUS ISO**
  - Canal d'annonce (email, téléphone, etc.)
  - Personne de contact ou de référence (évaluation du risque).
  - Informations à fournir : vol, perte, preuves, etc...



# BONNES MESURES

## Principaux risques

- **Télétravail**
  - Perte de confidentialité
  - Distraction

## Bonnes mesures pour éviter cela

- Aménager un espace de confidentialité (rester discret lors d'un téléphone ou visioconférence).
- Utiliser une liaison filaire serait mieux que Wifi.
- Sauvegarder les données professionnelles seulement sur le réseau de l'entreprise (VPN)

## Principaux risques

- **Déplacement et Voyages**
  - Perte et/ou vol de matériel
  - Risques dus à la connexion sur des réseaux étrangers (WiFi aéroport et hôtel)
  - - Problème d'alimentation électrique

## Bonnes mesures

- Posséder une liste de numéro d'urgence (police, ambassade, etc...)
- Faire contrôler le matériel au retour par le service informatique avant de le reconnecter au réseau

# BONNES MESURES (SUITE)

- Avoir une copie des numéros de série des terminaux, numéro IMEI (copie de factures)
- Activer la localisation des terminaux (avec un airTag par exemple)
- Ne jamais laisser aucun appareils sans surveillance



## Brochure de sécurité.

Il est conseillé de suivre les conseils expliqués à l'intérieur de l'ensemble de la brochure.

Avec les mesures citées ci-dessus, vous réduisez tout risques cités.