



Principaux risques

- **Messagerie**
 - **SPAM**
 - **Phishing**

- **Réseaux sociaux**
 - **Vol et usurpation d'identité**
 - **Désinformation, manipulation, contenus haineux**
 - **Cybersexisme, pornographie**
 - **E-réputation, cyberharcèlement, etc.**

© EPSIC 2021 – Tony Favre-Bulle – Module 231 – Appliquer la protection et la sécurité des données

3



Principales mesures et bonnes pratiques

Messagerie :

- **Apprendre à détecter les e-mails frauduleux (adresse inconnue, titre d'objet farfelu, fautes d'orthographe, liens hypertexte, etc.)**
- **S'informer des arnaques courantes (<https://www.votrepolice.ch>)**
- **Ne pas donner suite (répondre) à un e-mail suspect**
- **Annoncer l'arnaque (SCOCI → <https://www.ncsc.admin.ch>)**
- **Implémenter la signature électronique**

© EPSIC 2021 – Tony Favre-Bulle – Module 231 – Appliquer la protection et la sécurité des données

4



Principales mesures et bonnes pratiques

Réseaux sociaux :

- **Eviter de communiquer des données personnelles (date de naissance, No de téléphone, adresse physique, orientation religieuse, orientation politique, orientation sexuelle, état civil, affiliation, origine ethnique, etc.)**
- **Ne jamais utiliser le même pseudo (ou adresse e-mail) sur différents réseaux sociaux (tant pour l'identification que le nom de compte)**
- **Utiliser l'authentification à facteurs multiples**
- **Annoncer toute utilisation frauduleuse ou tentative d'abus (ne jamais minimiser les faits) (SCOCI → <https://www.ncsc.admin.ch>) et/ou à la police**

© EPSIC 2021 – Tony Favre-Bulle – Module 231 – Appliquer la protection et la sécurité des données