Principaux risques

- **Navigation Internet**
  - **Risque de perte d'anonymat (vol d'identité)**
  - **Traçage (marketing ou malveillant)**

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

- **Téléphonie**
  - **Smishing**

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

Principales mesures et bonnes pratiques

NAVIGATION INTERNET :

- **Mettre à jour le navigateur**
- **Utiliser les extensions disponibles (antivirus, blocage popup, filtre de sites douteux, géolocalisation, etc.)**
- **Ne transmettre aucune information sensible sur les forums, blogs et réseaux sociaux**
- **Lors d'échange de données bancaires, vérifier systématiquement que le protocole « https » (cadenas) est actif**
- **Effacer régulièrement l'historique (cookies, etc.)**
- **Utiliser la « navigation privée » sur les sessions publiques.**

Principales mesures et bonnes pratiques

Messagerie :

- **Apprendre à détecter les e-mails frauduleux (adresse inconnue, expéditeur inconnu, 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**

Principales mesures et bonnes pratiques

Téléphonie (SMS) :

- **En cas de doute, renseignez-vous sur des canaux officiels**
- **N'ouvrez aucun document et ne cliquez sur aucun lien si vous n'êtes pas sûr·e à 100% de l'expéditeur**
- **Vérifiez (Google) si la demande a déjà été identifiée comme une arnaque**
- **Supprimez le message**
- **Installez un logiciel antivirus et antispam sur votre smartphone Android**

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**