LA PROTECTION DES RENSEIGNEMENTS PERSONNELS PAR DES GESTES SIMPLES ET EFFICACES

AIDE-MÉMOIRE DE QUELQUES BONNES PRATIQUES

Ce document présente des actions qui, au quotidien, contribuent à renforcer le droit à la vie privée et permettent aux citoyennes et aux citoyens d'assurer un meilleur contrôle de leurs renseignements personnels. Les organismes publics pourront adapter et moduler ces actions selon leur réalité afin de répondre aux besoins de leur personnel et de leurs clientèles.

Comptes en ligne

Attention ! Soyez stratégique lors de la mise en place d'un processus d'authentification, et ce, pour diminuer les risques de vol de renseignements personnels.

- Activez l'authentification multifacteur, lorsque cette option est offerte.
- Créez des mots de passe robustes :
  - Évitez l'utilisation de renseignements personnels (ex. : date de naissance, nom d'un animal de compagnie, etc.);
  - Rehaussez-en la complexité (ex. : longueur, amalgame de lettres, de symboles et de chiffres, phrases, etc.);
  - Utilisez des mots de passe distincts d'une plateforme à une autre.
- Modifiez les mots de passe régulièrement.
- Conservez l'usage exclusif des mots de passe.
- Consultez régulièrement les différents comptes utilisés (ex. : institutions financières, cartes de crédit, achat en ligne, etc.) pour y repérer les anomalies et, le cas échéant, rapportez le tout aux organismes publics concernés.

Réception de correspondance et d'appels téléphoniques

Attention aux contacts malicieux, dont l'objectif est de se faire passer pour une personne digne de confiance.

- Ne répondez pas à une correspondance ni à un appel :
  - qui n'a pas été sollicité et qui demande des renseignements personnels ;
  - en provenance d'un organisme public qui ne communique généralement pas avec sa clientèle de cette façon ;
  - si, dans le cas d'un courriel, l'adresse et l'entête ne correspondent pas à la désignation habituelle de l'organisme public ;
  - dans le cas d'un courriel, dont l'expéditeur est inconnu ;
  - dont le message, dans le cas d'un courriel, est truffé de fautes (erreurs grammaticales et d'orthographe);
  - qui nécessite une action rapide, comme une invitation à profiter d'une offre valide pour une durée très limitée, pour laquelle l'interlocuteur insiste sur l'acceptation ;
  - qui réclame des paiements ou qui offre un remboursement ou de l'argent, alors qu'aucune transaction n'a été effectuée.
- En cas d'incertitude sur l'authenticité du message :
  - n'ouvrez pas les pièces jointes ;
  - ne cliquez pas sur les hyperliens ;
  - contactez l'organisme public en utilisant ses vraies coordonnées, et non celles qui y sont mentionnées ;
  - avisez les organismes publics concernés afin que ceux-ci puissent, le cas échéant, demander à leurs clientèles de se méfier des messages reçus en leur nom.

Web et médias sociaux

Attention aux arnaques, dont l'objectif est de soutirer de l'argent, des informations et des renseignements personnels en vue d'usurper l'identité d'une personne !

- Installez des logiciels antivirus et d'autres logiciels de protection et mettez-les à jour régulièrement.
- N'utilisez pas les réseaux Wi-Fi publics pour effectuer des consultations et des transactions qui impliquent des renseignements personnels (ex. : transactions bancaires, achats en ligne, consultation de dossiers auprès d'un organisme public, soumissions de formulaires Web), mais plutôt les sites sécurisés, dont l'adresse affiche un pictogramme de cadenas et débute par *https*.
- Ne divulguez pas de renseignements personnels sur les médias sociaux, car ces derniers pourraient être utilisés en vue d'un vol d'identité ou de fraude (ex. : date de naissance, adresse, numéro de téléphone, adresse courriel, numéro d'assurance sociale, pièce d'identité).
- Bloquez les contacts qui demandent de l'argent, des informations et des renseignements personnels.
- Limitez le nombre de personnes qui regardent les publications, en changeant les paramètres de confidentialité des médias sociaux utilisés.
- Portez une attention particulière aux pseudo concours, aux faux comptes et aux publications suspectes qui sollicitent des renseignements personnels.
- Désactivez les publicités ciblées.

Documents imprimés et électroniques

Attention ! La destruction de documents ou d'appareils électroniques doit se faire par un moyen sécuritaire.

- Lors de la destruction de documents imprimés qui contiennent des informations confidentielles et des renseignements personnels, utilisez un moyen, comme le déchiquetage sécurisé, qui ne permet pas, de manière réversible, une reconstitution des données.
- Détruisez les appareils électroniques (ex. : tablettes numériques, cellulaires, ordinateurs) qui contiennent des informations confidentielles et des renseignements personnels, notamment par un écrasement des données.