

Recommandations de sécurité relatives à l'utilisation d'internet

Mettre en place des mesures techniques

- ✓ Utiliser des mots de passe différents et sophistiqués
Eviter les noms ou prénom
Choisir des mots de passe d'au moins huit caractères (lettres, chiffres et caractères spéciaux)
Changer régulièrement les mots de passe
- ✓ Mettre régulièrement à jour les logiciels
- ✓ Installer et utiliser un logiciel antivirus et un pare-feu
- ✓ Faire régulièrement des sauvegardes de données importantes
- ✓ Veiller à toujours installer des applications mobiles depuis des sites de téléchargement officiels, valable également pour l'e-banking

Adopter un comportement prudent

- ✓ Prendre le temps d'analyser chaque message électronique reçu
- ✓ Se méfier de messages dont l'expéditeur n'est pas connu
- ✓ Vérifier la plausibilité du courrier électronique et être particulièrement attentif dès que la notion d'urgence ou de discrétion absolue est présente
- ✓ Ne pas cliquer machinalement sur les liens ou fichiers contenus dans le courrier électronique

Faire preuve de vigilance en naviguant sur internet

- ✓ Eviter les réseaux wi-fi publics pour effectuer des achats en ligne ou des opérations bancaires
- ✓ Fermer l'ensemble des sessions en se déconnectant via les fonctions prévues à cet effet et supprimer l'historique de navigation

Faire preuve de bon sens et d'esprit critique

- ✓ Ne pas donner suite lorsque l'on gagne à un jeu auquel on n'a pas joué
- ✓ Se méfier des héritages venant d'un parent éloigné, récemment décédé à l'étranger, mais inconnu (arnaque de type « faux héritage »). N'effectuer aucun versement préalable destiné à régler de prétendus frais de succession
- ✓ Se méfier des clés USB et disques durs externes lorsque leur provenance n'est pas connue, car ils peuvent contenir un virus informatique
- ✓ Ne **jamaïs** donner ses codes de cartes bancaires ou d'accès e-banking. Les prestataires bancaires ne demandent **jamaïs** ces informations.