1. Soyez prudent en utilisant Internet

- Naviguer sur des sites inconnus peut augmenter le risque d'être infecté de virus et d'autres codes indésirables.
- Téléchargez des documents et installez des programmes seulement lorsque le besoin s'en ressent et à partir de sources fiables.
- Ne partagez jamais des informations confidentielles ou personnelles si vous n'êtes pas sur de l'identité du destinataire ou si vous n'êtes pas sur que l'information en question est vraiment nécessaire.
- Ne partagez pas d'information sensible (ex PINs et mots de passe), même si vous êtes sure de la personne avec laquelle vous traitez. Si toutefois, vous avez une connexion internet sans fil, n'acceptez jamais de connexions à partir de réseaux sans fil avoisinants inconnus.

2. Soyez conscient du phishing

- Le phishing est une forme de tromperie conçue pour obtenir et user de vos données personnelles à des fins frauduleuses (tel que les numéros de votre carte de crédit, mots de passe et données du compte…)
- Des arnaqueurs peuvent envoyer des milliers de messages email frauduleux (ou même des Messages SMS) qui semblent provenir de sites web ou sources fiables, tel que votre banque ou compagnie de carte de crédit, vous demandant de donner des informations personnelles via email ou site web créés par eux à cet effet.
- Si vous recevez un émail ou message SMS suspect qui semble provenir de votre banque, veuillez procéder comme suit :
    - Ne répondez pas au message, ne cliquez sur aucun des liens et ne changez pas d'émail en aucun cas.
    - Contactez nous immédiatement
- N'entrez votre numéro de carte de crédit et données personnelles que lorsque la transaction est faite par vous-même et sur des sites web fiables
- Suivez régulièrement vos mouvements bancaires pour détecter des transactions frauduleuses.
- N'accédez pas à votre service « online Banking » dans des endroits ouverts, publics tel que Cyber Café
- Si vous utilisez des câbles modems ou DSL pour accéder à l'internet, ne laissez pas la connexion active lorsqu'elle n'est pas en utilisation, aussi pensez à installer un logiciel firewall personnel

3. Entretenir la Sécurité de votre Computer

- Réviser périodiquement la sécurité de votre computer, faire des réparations, mises à jour et remplacement appropriés.
- Entretenir votre computer est un élément important dans votre sécurité. l'un des moyens les plus efficaces pour protéger votre computer est l'utilisation d'un produit anti virus et antispyware.

4. Savoir comment répondre à un incident

- Apprendre à reconnaitre des incidents et savoir comment faire face si les choses vont mal
- Rappelez-vous qu'une réponse rapide peut être déterminante, ainsi si les choses vont réellement mal ou si vous rencontrez un événement suspect relatif à la sécurité, signalez le immédiatement
- Si vous ne savez pas comment rapporter un incident, appelez directement votre agence la plus proche.

5. Rappelez-vous que la Sécurité de l'Information est la Responsabilité de Chacun

En vous protégeant vous-même et les systèmes que vous utilisez, bien les utiliser et avec précaution : vous protégerez votre argent, votre vie privée et vos propres informations

6. Qu'est ce que l'Engineering Social (Manipulation Sociale)

- Le terme « Engineering Social » se réfère à l'art de manipuler des personnes pour contourner les systèmes de sécurité et effectuer une fraude.
- Cette technique vise à obtenir des informations par téléphone, fax, email traditionnel ou contact direct
- Comme moyen de lutter, adopter un comportement zen et ne délivrer aucune information pouvant vous compromettre
- Nonobstant le type d'information demandée, nous vous conseillons de :
  (1) Découvrir l'identité de l'interlocuteur en lui posons des questions précises (Nom, Prénom, Direction, N° de téléphone…)
  (2) Vérifier l'information fournie
  (3) Se poser la question sur l'importance de l'information demandée.

7. Email Canular

- Un email est « Canular » lorsqu'il semble provenir d'une source alors qu'il provient d'une toute autre source
- Un email canular est souvent une tentative de pousser l'utilisateur à faire un état désastreux ou à délivrer des informations importantes (tel que les mots de passe).
- Parmi les exemples, un email prétendant provenir de la banque demandant au client d'ouvrir un lien et d'entrer son numéro de carte de crédit, mot de passe internet ou PINs.
- A noter que lorsque la banque vous demande de changer votre mot de passe /PINs, elle ne spécifie pas la nature du changement ou vous envoyer un email avec un lien vous demandant de le changer.
- Aussi, une institution financière officielle ne vous demandera jamais de lui envoyer une information importante via un email, fax, téléphone, courrier postal ou tout autre moyen.

8. Sous Entendre les Mots de Passe et Authentification

- Les mots de passe ou toute autre méthode d'authentification comme Tokens sont des moyens que le système utilise pour vérifier si vous êtes réellement la personne que vous prétendez être.
- Si quelqu'un d'autre utilise votre login ou mot de passe par exemple, le système pensera qu'il s'agit de vous et cette personne peut tout faire à votre place (tel que des transactions)
- Ne révélez jamais vos mots de passe ou codes d'accès, ne les classer jamais dans un fichier non codé, ne les noter jamais sur papier sauf si vous les ranger dans un endroit fermé et sécurisé
- Les mots de passe doivent être compliqués et forts pour qu'ils soient difficiles à deviner ou craquer
- Utilisez des mots de passe compliqués comportant au moins 06 longs caractères et chiffres, lettres et caractères spéciaux

9. Sécurité de la Messagerie. Email et Messagerie Instantanée - Phishing encore une fois

- Email et messagerie instantanée sont des outils merveilleux mais peuvent être usés et abusés de différentes manières
- En règle générale, n'envoyez jamais d'informations confidentielles et importantes tel que les numéros de PIN, numéros de compte
- N'ouvrez pas un message jugé suspicieux, comportant un attachement inhabituel ou provenant d'un expéditeur inconnu.
- Rappelez vous qu'un émail est sujet à fourberie ou canular, s'assurer avant de juger que le message le message est bon
- Le phishing est une forme spéciale d'attaque où l'expéditeur envoie un faux message par exemple : (actuellement la banque actualise ses données et les clients sont invités à entrer dans leurs comptes et actualiser leurs références bancaires faute de quoi ce compte sera désactivé.) il dirigera le client vers un faux site web afin de récupérer ses informations bancaires (compte ou carte de crédit).