



## Le doute : votre meilleur allié

### Notes

#### Protégez vos informations personnelles

Ne donnez jamais de renseignements personnels par courriel, texto ou sur un site web qui semble frauduleux.

#### Faites vos mises à jour

En faisant régulièrement les mises à jour de vos systèmes d'exploitation, logiciels et applications mobiles, vous ajoutez un niveau de protection supplémentaire contre la fraude.

#### Signalez les messages frauduleux

Certains fraudeurs imitent les courriels et les textos de la Banque Nationale pour voler vos informations personnelles. En cas de doute, signalez le message.

#### Tapez directement dans la barre d'adresse

Pour accéder à notre site, prenez l'habitude de taper intégralement le [www.bnc.ca](http://www.bnc.ca) dans la barre d'adresse plutôt que d'utiliser un moteur de recherche.

#### Ne pas agir sous pression

Ne remettez jamais votre carte bancaire ni votre NIP à une personne disant travailler pour la Banque Nationale qui vient récupérer une carte défectueuse ou compromise à votre domicile.

#### Gardez vos mots de passe secrets

La Banque Nationale ne vous demande jamais votre mot de passe, que ce soit par texto, courriel ou par téléphone. Si une personne vous demande votre mot de passe, c'est forcément pour tenter une fraude. Ne communiquez jamais vos mots de passe.

#### Choisissez un mot de passe fort

Un mot de passe efficace est assez long (plus il s'approche des 21 caractères, plus il est fort). De plus, vous devriez utiliser un mot de passe différent pour chacun de vos services en ligne (courriel, compte en banque, réseaux sociaux, etc.).

#### Vérifiez les liens et l'expéditeur

Passez toujours votre souris au-dessus des liens contenus dans un courriel et vérifiez l'adresse de l'expéditeur. En cas de doute, ne cliquez pas sur les liens car c'est certainement une tentative de fraude.