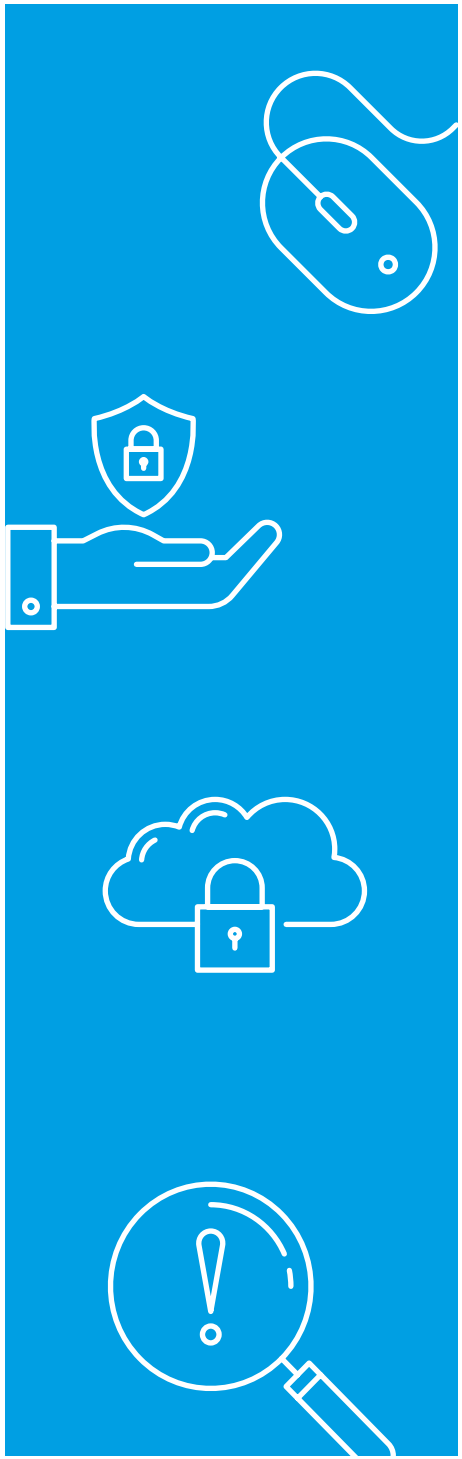
« 3D secure » ou « Pass sécurité » (selon votre banque).

Sur les réseaux sociaux (Facebook, Instagram...) restez discret, préférez l'anonymat !

- N'en dites pas trop de vous ! Ça n'intéresse pas que vos amis.
- Ne publier pas d'informations sur vos projets d'absences (vacances...).
- Divulguez uniquement les données absolument nécessaires.
- N'acceptez comme amis que les personnes que vous connaissez.

Que faire en cas de tentative de fraude (*phishing*, hameçonnage) ?

- Dénoncez les tentatives d'escroquerie ou de fraude sur **www.internet-signalement. gouv. fr**, sur **www.signal-spam.fr**
- Si vous recevez un SMS abusif, vous pouvez le transférer au numéro **33700**
- Pour toute question concernant l'usage de vos données personnelles, adressez-vous à la Commission nationale informatique et libertés (**www.cnil.fr**)
- En cas de fraude avérée, déposez votre plainte auprès de la police ou gendarmerie sur **www.pre-plainte-en-ligne.gouv.fr**



Ville de Fontenay-sous-Bois - Direction de la Communication - Studio graphique - Imprimerie - Ne pas jeter sur la voie publique

NAVIGUEZ SUR LE NET EN SÉCURITÉ !

www.fontenay.fr

Fontenay-sous-Bois
une ville à vivre

Vous utilisez un ordinateur (fixe ou portable), un téléphone mobile (*smartphone*), une tablette, et craignez de vous faire pirater vos données, de payer en ligne. Pour limiter ces risques, des bonnes pratiques suffisent parfois. En voici quelques-unes !

Ordinateur, *smartphone*, tablette : même combat !

- Installez un logiciel de sécurité anti-virus (et un seul) sur votre ordinateur.
- Vos appareils mobiles (smartphone, tablette) aussi sont vulnérables. Protégez-les également !

Mots de passe : faites preuve d'imagination !

- Si le service est proposé, connectez-vous depuis France connect ! Ainsi vous n'aurez pas à mémoriser un mot de passe supplémentaire.
- Prenez une phrase facile à retenir (exemple : « J'ai deux enfants qui s'appellent Laura et Tom »). Gardez uniquement la première lettre de chaque mot et les chiffres : « Ja2eqsaLeT », puis ajoutez un caractère spécial. « Ja2eqsaLeT@ »
- Gardez le même mot de passe et ajoutez les trois premières lettres du site sur lequel vous vous créez un compte. Exemple : sur Le Bon Coin : Ja2eqsaLeT@leb ; sur gmail : Ja2eqsaLeT@gmail
- Gardez vos mots de passe à l'abri : pas sous le clavier, ni dans un tiroir.
- Vos mots de passe n'appartiennent qu'à vous : **ne les communiquez jamais.** Si on vous interroge à ce sujet dans des e-mails ou au téléphone, ne répondez jamais à ces demandes. Les sociétés fiables ne vous demandent pas ce type d'information.
- Évitez de les enregistrer dans votre navigateur (Google Chrome, Firefox...)
- Sur votre tablette et *smartphone*, privilégiez le déverrouillage par reconnaissance faciale, empreinte ou iris.

Sauvegardes : l'atout sérénité.

- Pour préserver vos données, effectuez des sauvegardes régulières sur un support externe déconnecté (disque dur externe, clé USB) ou un service de stockage en ligne (*cloud*).

Wifi, clés USB, etc. : n'ouvrez pas la porte à n'importe qui !

- N'utilisez pas de clés USB inconnues.
- Faites installer votre wifi par un professionnel et remplacez le mot de passe par votre propre mot de passe. Ainsi, personne n'accèdera à votre réseau domestique.
- Ne vous connectez pas au wifi public ! Ces réseaux ne sont généralement pas cryptés.
- Déconnectez-vous ou supprimez votre compte lorsque vous n'en avez plus l'usage.
- Si vous partagez un ordinateur, déconnectez-vous de vos comptes personnels quand vous avez terminé.

Messagerie : méfiez-vous des apparences...

Les courriels, pièces jointes ou liens qu'ils contiennent réservent parfois de mauvaises surprises... Les incohérences de fond ou de forme (fautes d'orthographe, adresse mail de l'expéditeur douteuse) et les requêtes indiscrètes sont à prendre avec des pincettes.

- Ne cliquez jamais sur un lien ou une pièce-jointe si vous ne connaissez pas l'expéditeur.
- Ne répondez jamais à un courriel suspect. Au moindre doute, contactez l'expéditeur par un autre moyen et enregistrez son adresse mail dans les « indésirables »

Téléchargement : gare aux arnaques !

- Lorsque vous téléchargez des programmes et logiciels, préférez les sites officiels (et ceux de vos fournisseurs). Ne téléchargez pas de logiciels inconnus.
- Sachez que les démarches administratives d'État (carte grise, extrait d'acte de naissance...) sont gratuites sur les sites officiels gouvernement.fr, service-public.fr

Mises à jour : ne les remettez pas au lendemain !

- Les mises à jour des logiciels permettent de pallier les failles de sécurité. Mettez-les à jour à chaque fois que vos ordinateur, smartphone, tablette ou un programme que vous utilisez vous le proposent. Ils seront moins vulnérables.

Paiement en ligne : évitez les frais !

- Effectuez vos paiements sur des sites sécurisés : ils commencent par « https : » et ont un cadenas dans la barre d'adresse. Exemple :

- Ne communiquez jamais votre n° de carte de paiement.
- Certains site marchands vous proposent d'enregistrer votre carte bancaire pour un usage ultérieur. Ne le faites que si c'est un site où vous avez l'habitude d'acheter !
- Activez la vérification en deux étapes proposée par votre banque. Ainsi, vous serez invités à confirmer votre paiement grâce à un code de validation envoyé par SMS ou par appel, ou grâce à une notification qui apparaît sur votre smartphone ou tablette, exemple « Sécur pass »,