

FICHE RÉSUMÉE

USAGES ET BONNES PRATIQUES DE SÉCURITÉ

Pourquoi se protéger ?



Les premiers remparts : le mot de passe :

Petits rappels



Un mot de passe solide :
8 caractères minimum
mais 12 c'est mieux



Ne pas toujours utiliser le même
On peut utiliser un gestionnaire de mot de passe



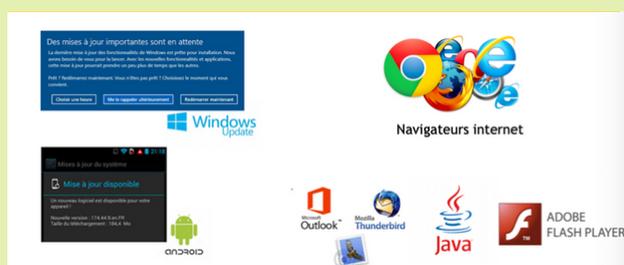
Ne jamais le communiquer

Avoir un antivirus et un pare feu à jour :



Des versions payantes ou gratuites
Sur son ordinateur mais aussi sur ses
appareils mobiles
Faire des scans et des mises à jour
régulièrement
Le Pare Feu ou Firewall filtre les
données qui entrent ou sortent de
l'ordinateur

Avoir un ordinateur et ses logiciels à jour :



Les virus et le vol de données passent par les mails :

Soyez attentif à l'expéditeur.
Regardez l'heure d'envoi.
Ne communiquez JAMAIS vos identifiants, mots de passe et numéros bancaires.
Ne cliquez jamais sur un lien dans le message.
Ne pas ouvrir une pièce jointe d'un expéditeur inconnu.
Privilégiez Cci à A pour l'envoi de mail à plusieurs expéditeur



Être attentif aux téléchargement :



Effectuer des sauvegardes régulières :



Les règles a respecter pour le paiement en ligne :



Les règles à respecter pour le paiement en ligne :

Vérifiez que la page est bien sécurisée

Prenez garde aux sites inconnus ou « exotiques »



Info Escroqueries

Pour se renseigner sur les escroqueries ou pour signaler un site internet ou un courriel d'escroqueries, un vol de coordonnées bancaires ou une tentative de hameçonnage

Par téléphone

0 805 805 817

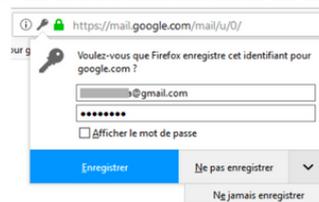
Du lundi au vendredi de 9h à 18h30.

Numéro vert (appel gratuit).

Vérifiez que la page est bien sécurisée

Prenez garde aux sites inconnus ou « exotiques »

Évitez d'enregistrer vos coordonnées bancaires ou vos mots de passe



Vérifiez que la page est bien sécurisée

Prenez garde aux sites inconnus ou « exotiques »

Évitez d'enregistrer vos coordonnées bancaires ou vos mots de passe

Utilisez les solutions proposées par les banques



ou des comptes type Paypal



Utiliser un réseau sans fil bien sécurisé :

Avoir un protocole de cryptage et un mot de passe solide

Filtrer les adresses Mac

MOD FIBRE 11 SAGEM MIXXW
Modèle: FIB@T1 20M DC
PIN: 253637418
S/N: NQZ500129000001
CM MAC: 001E1E1000001
B/F/A MAC: 001E1E1000004

Configuration Accès
192.168.0.1 ou
192.168.0.254
Login: admin
Password: admin@1234

SAGEMCOM
CE
MADE IN CHINA

Nom du réseau SSID: XXXX-abcd
Clé de sécurité Wi-Fi: aedfghijklm
Accès configuration modem

nom équipement	adresse IP	adresse MAC	statut	supprimer
android-02	192.168.1.11	94:68:59:30:aa:59	bloqué	<input type="checkbox"/>
cd-46:97:24:16:16		cd-46:97:24:16:24	libre	<input type="checkbox"/>
iPhone/Nostr	192.168.1.22	89:6d:24:89:18:18	libre	<input type="checkbox"/>

Avant tout, des réflexes simples :

Se déconnecter

Régler ses paramètres de confidentialité

Être prudent lorsque l'on saisit des données sur son smartphone ou son ordinateur

Effacer ses données ou utiliser la navigation privée sur un appareil qui n'est pas le vôtre

Ne cliquez pas sur n'importe quel lien et ne répondez pas à des mails ou SMS bizarres