

Mot de passe



Il est **complexe**

Il ne dit rien de vous

Un compte = un mot de passe

Ne traîne jamais sur papier

2 protections valent mieux qu'une

Méfiance



Les « faux »
logiciels



Télécharger uniquement sur les sites officiels ou les magasins (Playstore, Appstore)



L'hameçonnage
(phishing)

Ne cliquer jamais sur un mail ou lien inconnu.

Analyser toujours les contenus de mails ou de sms avant d'agir



Site d'achat
frauduleux

Assurez-vous d'être bien dans le cas d'un achat sécurisé (cadenas + https + mentions légales et conditions générales de vente)

@-réputation



La @-réputation ou réputation sur internet correspond à l'image que les internautes se font sur un sujet par les informations trouvées sur le web via les moteurs de recherche, les réseaux sociaux, les blogs, les forums...

Sauvegarde



Faire une sauvegarde c'est avoir le même élément à 2 endroits bien distincts !

Mise à jour

Avoir un équipement à jour, c'est garantir que les failles découvertes par le fabricant soient corrigées

Protection

Avoir un antivirus, c'est protéger votre équipement numérique des virus.



Un virus est un programme qui altère le fonctionnement normal de votre ordinateur

Prudence

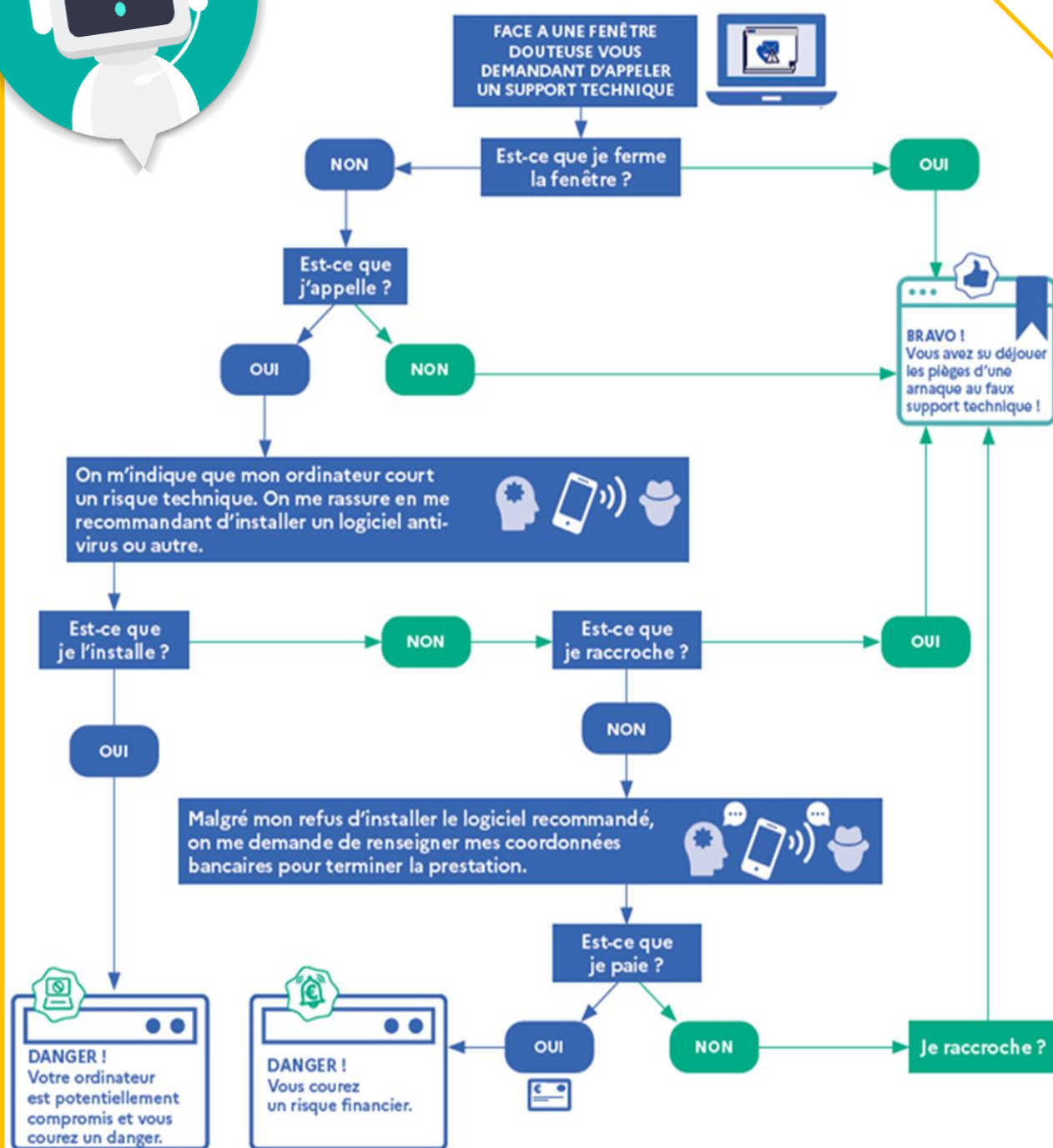


Quand on se connecte à un Wi-Fi public, comme son nom l'indique, on ne peut pas connaître tous les utilisateurs, il faut donc rester prudent.



= Risques = Prudence

Sur un wifi public, je ne fais rien de personnel, je consulte uniquement des informations, sans saisie de mes identifiants personnels (mot de passe ou bancaires)



Victime d'hameçonnage

Si vous avez malencontreusement communiqué des informations sensibles, comme votre numéro de carte bancaire, **déposez plainte au commissariat de police ou à la gendarmerie la plus proche**. Les cybercriminels pourraient, en effet, en faire un usage frauduleux. Pour être conseillé **en cas d'hameçonnage**, contactez le service Info Escroqueries au **0805 805817** (appel gratuit).