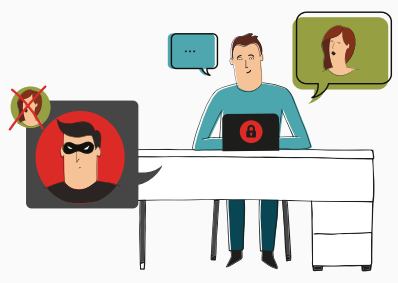
NOS CONSEILS POUR VOTRE SÉCURITÉ NUMÉRIQUE

ADOPTEZ LES BONNES PRATIQUES

Les mots de passe

Choisissez une mot de passe long, complexe, impossible à deviner et différent pour chaque service mélangeant majuscules, minuscules, chiffres et caractères spéciaux

La sécurité sur les réseaux sociaux

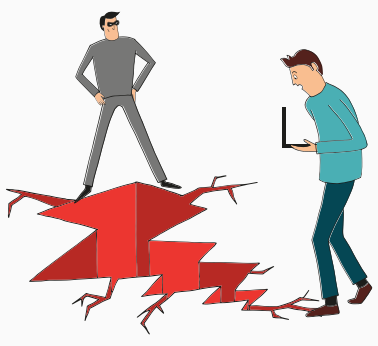


Vérifiez vos paramètres de confidentialité et maîtrisez vos publications

Les sauvegardes

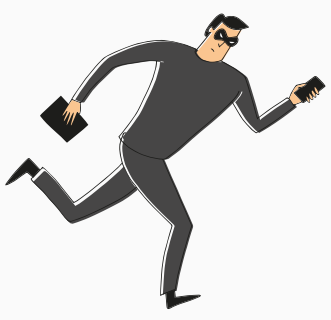
Sauvegardez régulière-ment vos données et veillez à tester vos sauvegardes

Les mises à jour



Mettez régulièrement à jour vos appareils et vos logiciels depuis les sites officiels

La sécurité des appareils mobiles

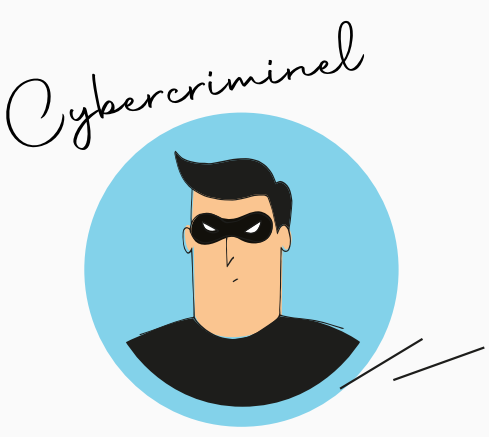


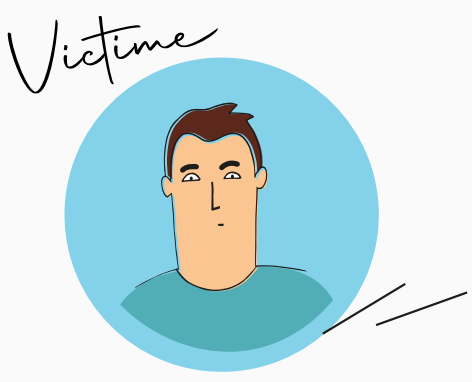
Évitez les Wi-Fi publics, privilégiez les Wi-Fi sécurisés et mettez en place des codes d'accès

Les usages PRO-PERSO

Utilisez un mot de passe différent pour vos services professionnels et personnels

COMPRENDRE LES RISQUES ET RÉAGIR





L'HAMEÇONNAGE (PHISHING)

Vous recevez un message ou un appel inattendu, voire alarmant, d'une organisation connue et d'apparence officielle qui vous demande des informations personnelles ou bancaires ?

Vous êtes peut-être victime d'une attaque par hameçonnage

- Ne communiquez jamais d'informations sensibles suite à un message ou un appel téléphonique
- Au moindre doute, contactez directement l'organisme concerné pour confirmer
- Changez immédiatement vos mots de passe

LES RANÇONGICIELS (RANSOMWARE)

Vous ne pouvez plus accéder à vos fichiers et on vous demande une rançon ?

Vous êtes victime d'une attaque par rançongiciel

- Débranchez la machine d'Internet et du réseau local
- Ne payez pas la rançon, déposez plainte
- Faites-vous assister par des professionnels pour identifier et corriger l'origine de l'infection
- Restaurez les données

L'ARNAQUE AU FAUX SUPPORT TECHNIQUE

Votre ordinateur est bloqué et on vous demande de rappeler un support technique ?

Vous êtes victime d'une arnaque au faux support

- Conservez toutes les preuves
- Redémarrez votre appareil
- Purgez le cache, supprimez les cookies, réinitialisez les paramètres de votre navigateur, puis faites une analyse antivirus
- Désinstallez tout nouveau programme suspect
- Changez tous vos mots de passe

POUR PLUS DE CONSEILS ET D'ASSISTANCE, RENDEZ-VOUS SUR :
www.cybermalveillance.gouv.fr