RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

LES ESSENTIELS DE VOTRE SÉCURITÉ NUMÉRIQUE

LES MENACES

COMMENT RÉAGIR SI VOUS ÊTES VICTIME ?

L'HAMEÇONNAGE

VOL DE DONNÉES

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 (*phishing*) !

- **NE COMMUNIQUEZ JAMAIS** d'information sensible suite à un message ou un appel téléphonique
- Au moindre doute, **CONTACTEZ DIRECTEMENT L'ORGANISME** concerné pour confirmer
- **FAITES OPPOSITION** immédiatement (en cas d'arnaque bancaire)
- **CHANGEZ VOS MOTS DE PASSE** divulgués/compromis
- **DÉPOSEZ PLAINTE**
- **SIGNALEZ-LE** sur les sites spécialisés

LES RANÇONGICIELS

EXTORSION D'ARGENT

Vous ne pouvez plus accéder à vos fichiers et on vous demande une rançon ? Vous êtes victime d'une attaque par rançongiciel (*ransomware*) !

- **DÉBRANCHEZ LA MACHINE D'INTERNET** et du réseau local
- En entreprise, **ALERTEZ LE SUPPORT INFORMATIQUE**
- **NE PAYEZ PAS** la rançon
- **DÉPOSEZ PLAINTE**
- **IDENTIFIEZ ET CORRIGEZ** l'origine de l'infection
- Essayez de **DÉSINFECTER LE SYSTÈME** et de déchiffrer les fichiers
- **RÉINSTALLEZ LE SYSTÈME** et restaurez les données
- **FAITES-VOUS ASSISTER** par des professionnels

L'ARNAQUE AU FAUX SUPPORT TECHNIQUE

ESCROQUERIE FINANCIÈRE

Votre ordinateur est bloqué et on vous demande de rappeler un support technique ? Vous êtes victime d'une arnaque au faux support !

- **NE RÉPONDEZ PAS**
- **CONSERVEZ** toutes les preuves
- **REDÉMARREZ** votre appareil
- **PURGEZ LE CACHE**, supprimez les cookies et réinitialisez
- les paramètres de votre navigateur
- **DÉSINSTALLEZ** tout nouveau programme suspect
- Faites une **ANALYSE ANTIVIRUS**
- **CHANGEZ TOUS VOS MOTS DE PASSE**
- **FAITES OPPOSITION** auprès de votre banque si vous avez payé
- **DÉPOSEZ PLAINTE**

LE PIRATAGE DE COMPTE

VOL DE DONNÉES

Vous constatez une activité anormale ou inquiétante sur vos comptes ou applications (messagerie, réseaux sociaux, sites administratifs, banques, sites e-commerce…) ? Vous êtes peut-être victime d'un piratage de compte !

- **CHANGEZ VOTRE MOT DE PASSE** piraté sur tous les sites ou comptes sur lesquels vous pouviez l'utiliser
- **VÉRIFIEZ** que les coordonnées de récupération de votre compte (e-mail, téléphone) n'ont pas été modifiées
- **PRÉVENEZ VOTRE BANQUE**
- **PRÉVENEZ TOUS VOS CONTACTS** de ce piratage
- **SAUVEGARDEZ** les preuves
- **DÉPOSEZ PLAINTE** si le préjudice le justifie

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

✓ LES **BONNES PRATIQUES**

LES MOTS DE PASSE

Votre mot de passe doit être différent pour chaque service, suffisamment long et complexe, et impossible à deviner. Ne le communiquez jamais à un tiers. Pour votre messagerie, il doit être particulièrement robuste.

LA SÉCURITÉ SUR LES RÉSEAUX SOCIAUX

Protégez l'accès à vos comptes, vérifiez vos paramètres de confidentialité et maîtrisez vos publications. Faites attention à qui vous parlez. Vérifiez régulièrement les connexions à votre compte.

LES SAUVEGARDES

Pour éviter de perdre vos données, effectuez des sauvegardes régulières. Identifiez les appareils et supports qui contiennent des données et déterminez lesquelles doivent être sauvegardées. Choisissez une solution adaptée à vos besoins. Protégez et testez vos sauvegardes.

LES MISES À JOUR

Mettez à jour sans tarder l'ensemble de vos appareils et logiciels. Téléchargez les mises à jour uniquement depuis les sites officiels et activez l'option de téléchargement et d'installation automatique des mises à jour.

PLUS D'INFORMATIONS SUR **WWW.CYBERMALVEILLANCE.GOUV.FR**