RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR

Assistance et prévention en sécurité numérique

LES ESSENTIELS DE VOTRE SÉCURITÉ NUMÉRIQUE

LES MENACES

L'HAMEÇONNAGE

VOL DE DONNÉES

Vous recevez un message ou un appel inattendu, voire alarmant, d'apparence officielle qui vous demande des informations personnelles ou bancaires ? Vous êtes peut-être victime d'une tentative d'hameçonnage (*phishing*) !

LES RANÇONGICIELS

EXTORSION D'ARGENT

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

L'ARNAQUE AU FAUX SUPPORT TECHNIQUE

ESCROQUERIE FINANCIÈRE

Un message d'alerte s'affiche sur votre ordinateur qui semble bloqué ? Ce message vous incite à appeler d'urgence un numéro de support (Microsoft, Apple…) ? Vous êtes victime d'une arnaque au faux support !

LE PIRATAGE DE COMPTE

VOL DE DONNÉES

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

COMMENT RÉAGIR SI VOUS ÊTES VICTIME ?

- **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 (33700, Signal Spam…)

- **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
- Sinon, **RÉINSTALLEZ LE SYSTÈME** et restaurez les données
- **FAITES-VOUS ASSISTER** par des professionnels

- **N'APPELEZ PAS** le numéro
- **CONSERVEZ** toutes les preuves
- **REDÉMARREZ** votre appareil
- **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**
- Au besoin, **FAITES-VOUS ASSISTER** par des professionnels

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

LES BONNES PRATIQUES

LES MOTS DE PASSE

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

LES SAUVEGARDES

Pour ne pas perdre vos données, sauvegardez-les régulièrement. Pour chacun de vos appareils (ordinateurs, tablette, téléphone…), déterminez les données à sauvegarder. Déconnectez votre support de sauvegarde après utilisation. Protégez et testez vos sauvegardes.

LES MISES À JOUR

Mettez à jour sans tarder tous vos appareils et logiciels. Ne téléchargez les mises à jour que depuis les sites officiels. Activez le téléchargement et l'installation automatique des mises à jour.

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.

PREMIER MINISTRE

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE

MINISTÈRE DE L'INTÉRIEUR ET DES OUTRE-MER

MINISTÈRE DE L'ÉDUCATION NATIONALE ET DE LA JEUNESSE

MINISTÈRE DES ARMÉES

MINISTÈRE DE LA JUSTICE

SECRÉTARIAT D'ÉTAT CHARGÉ DU NUMÉRIQUE

Plus de conseils et d'assistance sur www.cybermalveillance.gouv.fr