CYBER CRIMINALITÉ

Les essentiels

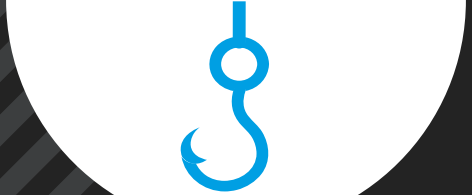
Connaître

LES MENACES

Savoir

COMMENT RÉAGIR

Les bonnes pratiques



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)* !

Source : GIP ACYMA - Cybermalveillance.gouv.fr

L'hameçonnage

Comment réagir ?

1. Ne communiquez jamais d'information sensible suite à un message ou un appel téléphonique
2. Au moindre doute, contactez directement l'organisme concerné
3. Faites opposition immédiatement (en cas d'arnaque bancaire)
4. Changez vos mots de passe divulgués/compromis
5. Déposez plainte
6. Signalez-le sur les sites spécialisés

SOREX | Expertise-Comptable & Audit | www.sorex.pro
Source : GIP ACYMA - Cybermalveillance.gouv.fr

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)* !

Source : GIP ACYMA - Cybermalveillance.gouv.fr

Les rançongiciels

Comment réagir ?

1. Débranchez la machine d'Internet et du réseau local
2. En entreprise, alertez le support informatique
3. Ne payez pas la rançon
4. Déposez plainte
5. Identifiez et corrigez l'origine de l'infection
6. Essayez de désinfecter le système et de déchiffrer les fichiers
7. Réinstallez le système et restaurez les données
8. Faites-vous assister par des professionnels

SOREX | Expertise-Comptable & Audit | www.sorex.pro
Source : GIP ACYMA - Cybermalveillance.gouv.fr

L'arnaque 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 !

SOREX | Expertise-Comptable & Audit | www.sorex.pro
Source : GIP ACYMA - Cybermalveillance.gouv.fr

L'arnaque technique

Comment réagir ?

1. Ne répondez pas et conservez toutes les preuves
2. Redémarrez votre appareil
3. Purgez le cache, supprimez les cookies et réinitialisez les paramètres de votre navigateur
4. Désinstallez tout nouveau programme suspect
5. Faites une analyse antivirus
6. Changez tous vos mots de passe
7. Faites opposition à la banque si vous avez payé
8. Déposez plainte

SOREX | Expertise-Comptable & Audit | www.sorex.pro
Source : GIP ACYMA - Cybermalveillance.gouv.fr

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 !

Source : GIP ACYMA - Cybermalveillance.gouv.fr

Le piratage de compte

Comment réagir ?

1. Changez votre mot de passe piraté sur tous les sites ou comptes sur lesquels vous pouviez l'utiliser
2. Vérifiez que les coordonnées de récupération de votre compte (e-mail, téléphone) n'ont pas été modifiées
3. Prévenez votre banque
4. Prévenez tous vos contacts de ce piratage
5. Sauvegardez les preuves
6. Déposez plainte si le préjudice le justifie

SOREX | Expertise-Comptable & Audit | www.sorex.pro
Source : GIP ACYMA - Cybermalveillance.gouv.fr

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.

Source : GIP ACYMA - Cybermalveillance.gouv.fr

Les bonnes pratiques

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.

Source : GIP ACYMA - Cybermalveillance.gouv.fr

Les bonnes pratiques

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 bonnes pratiques

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.

Source : GIP ACYMA - Cybermalveillance.gouv.fr