csm
www.cybersecurite-management.fr

Nos conseils pour **votre sécurité numérique**

Adopter 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.

LA SÉCURITÉ DES APPAREILS MOBILES
Mettez en place les codes d'accès. Appliquez les mises à jour de sécurité et faites des sauvegardes, évitez les réseaux Wi-Fi publics ou inconnus. Ne laissez pas votre appareil sans surveillance.

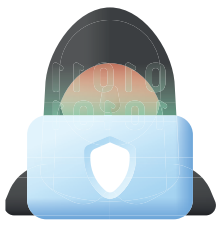
LES SAUVEGARDES
Pour éviter de perdre vos données, effectuez des sauvegardes régulières. Identifiez les appareils et supports qui contiennent des données et déterminez lesquelles doivent être sauvegardées. Choisissez une solution adaptée à vos besoins. Protégez et testez vos sauvegardes.

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.

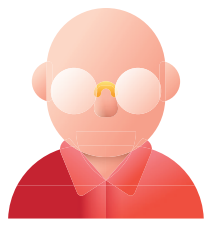
LES USAGES PRO-PERSO
Utilisez des mots de passe différents pour tous les services professionnels et personnels auxquels vous accédez. Ne mélangez pas votre messagerie professionnelle et personnelle et n'utilisez pas de service de stockage en ligne personnel à des fins professionnelles.

Comprendre les risques et réagir

LES RISQUES



COMMENT RÉAGIR ?



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* en anglais) !

BUT
Voler des informations personnelles ou professionnelles (identité, adresses, comptes, mots de passe, données bancaires…) pour en faire un usage frauduleux.

TECHNIQUE
Leurre envoyé via un faux message, SMS ou appel téléphonique d'administrations, de banques, d'opérateurs, de réseaux sociaux, de sites d'e-commerce…

- 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'anarques bancaires)
- Changez vos mots de passe divulgés/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*, en anglais) !

BUT
Réclamer le paiement d'une rançon pour rendre l'accès aux fichiers verrouillés.

TECHNIQUE
Blocage de l'accès à des données par envoi d'un message contenant des liens ou pièces jointes malveillantes ou par intrusion sur le système.

- Débranchez la machine d'Internet et du réseau local
- En entreprise, alertez le support informatique
- Ne payez pas la rançon
- Déposez plainte
- Identifiez et corriger 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 !

BUT
Inciter la victime à payer un pseudo dépannage informatique et/ou la faire souscrire à des abonnements payants

TECHNIQUE
Faire croire à un problème technique grave impliquant un risque de perte de données ou d'usage de l'équipement (par écran bloqué, téléphone, SMS, courriel, etc.).

- 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

https://cybersecurite-management.fr