Hameçonnage : 5 réflexes

SMS, e-mails, appels : les arnaques se font passer pour des organismes de confiance.

1. Méfiez-vous de l'urgence : « colis bloqué », « compte suspendu », « amende à régler sous 24 h ».
2. Ne cliquez pas : tapez vous-même l'adresse du site officiel ou ouvrez son application.
3. Vérifiez l'expéditeur et l'adresse exacte du site avant de saisir quoi que ce soit.
4. Ne donnez jamais un mot de passe, un code reçu par SMS ou votre carte bancaire suite à un message.
5. Signalez : SMS au 33700, e-mail sur signal-spam.fr.

Un lien vous semble louche ?

Vérifiez-le sans cliquer :
infonewscyber.fr/verifier-un-lien

Besoin d'aide ?

17cyber.gouv.fr · assistance gratuite

Affiche libre de diffusion (CC BY 4.0) · InfoNews Cyber

Mots de passe : les bons réflexes

***

Un mot de passe volé ouvre la porte à tous les comptes qui l'utilisent.

1. Un mot de passe différent pour chaque compte, sans exception.
2. Long : au moins 12 caractères, ou une phrase de passe de 4 ou 5 mots.
3. Un gestionnaire de mots de passe les crée et les retient pour vous.
4. Activez la double authentification sur la messagerie, la banque et les réseaux sociaux.
5. Ne le communiquez à personne, même à un « support technique » qui vous appelle.

Votre mot de passe a-t-il fuité ?

Vérifiez-le en toute confidentialité :
infonewscyber.fr/mot-de-passe

Besoin d'aide ?

17cyber.gouv.fr · assistance gratuite

Affiche libre de diffusion (CC BY 4.0) · InfoNews Cyber

Faux conseiller bancaire : raccrochez !

L'escroc appelle avec le vrai numéro de votre banque et parle de fraude sur votre compte.

1. Votre banque ne vous demandera jamais un code reçu par SMS.
2. Ni de valider une opération dans l'application pour « l'annuler ».
3. Le numéro qui s'affiche peut être falsifié : ce n'est pas une preuve.
4. Raccrochez, puis rappelez vous-même le numéro au dos de votre carte.
5. Victime ? Faites opposition sur votre carte et portez plainte.

Les gestes en cas de fraude bancaire :

Le guide pas à pas :
infonewscyber.fr/guide/fraude-bancaire

Besoin d'aide ?

17cyber.gouv.fr · assistance gratuite

Affiche libre de diffusion (CC BY 4.0) · InfoNews Cyber

Cyberattaque : les premiers gestes

Écran bloqué, fichiers illisibles, demande de rançon : chaque minute compte.

1. Débranchez l'ordinateur du réseau (câble et Wi-Fi), sans l'éteindre.
2. Prévenez tout de suite votre responsable informatique ou votre prestataire.
3. Ne payez pas la rançon : rien ne garantit le retour de vos données.
4. Gardez les preuves : messages, captures d'écran, fichiers modifiés.
5. Faites-vous aider sur 17cyber.gouv.fr et portez plainte.

Toutes les étapes, pour les entreprises :

Le guide complet :
infonewscyber.fr/guide/rancongiciel-entreprise

Besoin d'aide ?

17cyber.gouv.fr · assistance gratuite

Affiche libre de diffusion (CC BY 4.0) · InfoNews Cyber