60 Anos Setronix desde 1966

OCTOBRE
2026
2e QUINZAINE | PRÉVENTION



CYBERSÉCURITÉ
ARRÊTEZ ET VÉRIFIEZ

Un message urgent doit aussi être vérifié.

1. Dangers et risques

Dangers : Faux messages, pièces jointes et liens suspects.

Risques : Vol de données, fraude et accès non autorisé aux comptes.

2. Avant de commencer

- Vérifiez l'adresse complète de l'expéditeur.
- Confirmez les demandes via un contact déjà connu.
- Utilisez uniquement les applications et canaux autorisés.

3. Arrêtez et signalez

- Demande de mot de passe ou de code d'accès.
- Urgence, secret ou changement de coordonnées bancaires.
- Vous avez cliqué ou envoyé des données ? Signalez-le immédiatement.

4. Comment agir : quatre étapes de prévention

1 

Lisez
Vérifiez l'expéditeur et le contexte.

2 

Confirmez
Utilisez un contact indépendant.

3 

Protégez
Ne partagez ni identifiants ni codes.

4 

Signalez
Utilisez le canal interne prévu.

5. Choisissez la mesure de prévention adaptée

Situation	Mesure de prévention
E-mail / SMS	N'ouvrez aucun lien ni pièce jointe sans en vérifier l'origine.
Demande de paiement	Validez tout changement par un autre canal déjà connu.
Comptes / identifiants	Un mot de passe distinct par compte ; activez la MFA si disponible.
Incident possible	Conservez le message ; suivez les consignes du support informatique.

Bonnes pratiques : Ne vous fiez pas uniquement au nom affiché ou à l'apparence du message. L'authentification multifacteur (MFA) renforce la protection ; ne partagez jamais ses codes.

6. ACTION DE LA QUINZAINE Face à un message inattendu, vérifiez son origine avant de cliquer. Identifiez le canal interne pour signaler un doute.

LISEZ • CONFIRMEZ • PROTÉGEZ • SIGNALEZ

CNCS : bonnes pratiques CNCS : mots de passe