Cybersécurité

As-tu le déclic avant de répondre à une demande urgente ou sensible?

Une demande urgente ou sensible peut sembler légitime, même lorsqu'elle ne l'est pas. Avant de cliquer, de répondre, de transmettre un code ou de partager de l'information, prenez un moment pour vérifier.

Les trois gestes à retenir

1 Repérez et signalez les signes suspects

Soyez attentif aux :

- demandes urgentes ou inhabituelles;
- demandes d'information sensible;
- adresses réelles d'expéditeurs qui ne correspondent pas au nom affiché;
- liens, pièces jointes ou codes QR inattendus;
- messages qui exercent de la pression pour agir rapidement.

En cas de doute, signalez le message selon les mécanismes prévus dans votre organisation afin de permettre aux équipes responsables d'intervenir.

Questions à se poser

Est-ce que je repère un signe suspect? Si oui, est-ce que je l'ai signalé?

2 Validez la demande par un autre moyen

Avant de répondre à un message qui vous semble suspect, confirmez la demande par un moyen de communication fiable et distinct du message reçu, par exemple :

- par téléphone;
- dans Teams;
- en personne.

Question à se poser

Est-ce que j'ai confirmé la demande par un autre moyen auprès de la bonne personne?

3 Activez l'authentification multifacteur lorsque possible

L'authentification multifacteur ajoute une protection supplémentaire à vos comptes et peut aider à bloquer une tentative d'accès non autorisée, même si votre mot de passe est compromis.

- Activez-la lorsque possible.
- Approuvez uniquement les demandes d'authentification que vous avez effectuées.
- Signalez toute demande d'authentification inattendue ou répétée.
- Changez votre mot de passe.

Question à se poser

Ai-je reçu une demande d'authentification que je n'ai pas effectuée?

As-tu le déclic?

Québec