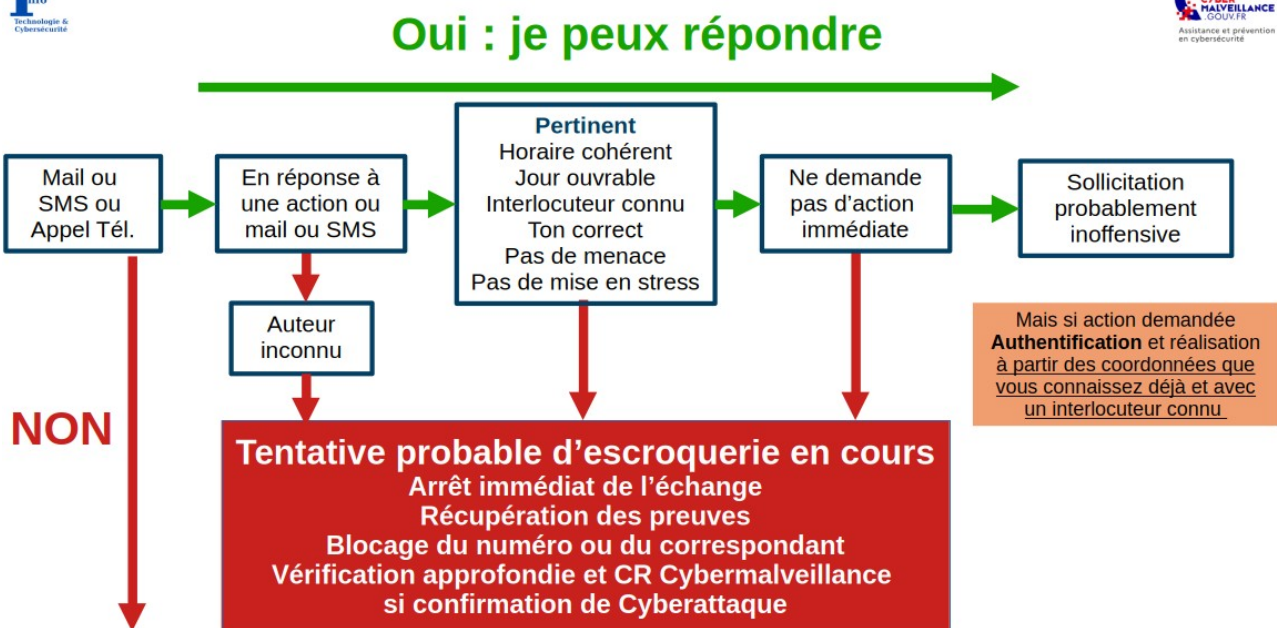


Ne pas être victime d'une attaque par socio engineering

1. **Ne jamais répondre à un mail, un SMS/RCS, message sur un réseau social, WhatsApp ou à un appel d'origine inconnue.** Pour les appels et en cas d'un correspondant sérieux, il laissera au moins un message.
2. **Après avoir répondu à un appel d'un correspondant supposé CONNU, exigez que le correspondant se présente** (ou identifiez le de façon indirecte) et au moindre doute sur l'identité de la personne (voix différente, vocabulaire, débit...), écoutez la conversation, attendez quelques minutes et rappelez sur un numéro connu (ne pas faire rappel du dernier numéro) pour avoir une certitude.
3. **Ne jamais cliquer sur un lien prétendant aller sur un site, proposant un paiement, quelque que ce soit le support.** Si le correspondant est inconnu, vous ignorez, sinon, identifiez clairement l'origine et accédez au site par la procédure que vous utilisez normalement pour avoir de plus amples informations.
4. **Ne pas se laisser aguicher par des offres trop bon marché, vérifier la réputation des sites de ventes sur lesquels vous voulez effectuer une transaction.** Au moindre doute : pas de transaction.

Le schéma ci-dessous vous aidera à décider si vous êtes victime d'une tentative d'escroquerie.



5. **Ne donnez jamais vos mots de passe, vos identifiants, ne partagez jamais votre écran, ne donnez jamais la main sur votre terminal à un intervenant inconnu.** En cas de doute clôturez la session et vérifiez.
6. **Ne pas donner à des inconnus et ne pas mettre en ligne (statut, réseau sociaux, répondants...) des informations qui permettent d'en savoir trop sur vous, sur vos proches et sur vos activités.**

<https://www.cybermalveillance.gouv.fr> qui pourra vous proposer une assistance.