

J'ai cliqué sur un lien suspect

Email, SMS ou QR code frauduleux : les bons gestes dans les 10 minutes.

1 Ne rien saisir de plus

Fermez la page. Si vous avez déjà saisi un mot de passe, passez immédiatement à l'étape 2.

2 Changer le mot de passe concerné

Depuis un autre onglet, en tapant vous-même l'adresse du service. Changez-le aussi partout où il est réutilisé.

3 Activer la double authentification

Sur le compte touché, si ce n'était pas déjà fait.

4 Débrancher si un fichier a été ouvert

Pièce jointe ou téléchargement ouvert : débranchez le câble réseau et coupez le Wi-Fi — sans éteindre l'ordinateur.

5 Prévenir, sans honte

Signalez immédiatement au référent informatique. Signaler vite est un bon réflexe, jamais une faute.

6 Surveiller

Coordonnées bancaires saisies ? Appelez la banque et surveillez les comptes. Conservez le message frauduleux comme preuve.

À retenir

La règle d'or : jamais d'identifiants ni de codes saisis depuis un lien reçu. En cas de doute, on ne clique pas, on signale.

Assistance Cyberionis : 06 64 90 07 74 · contact@cyberionis.fr · cyberionis.fr