

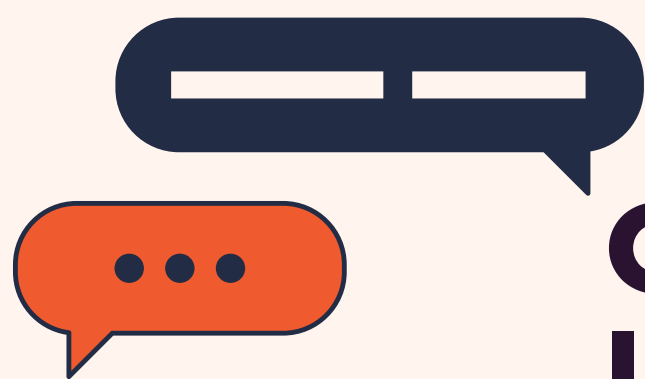
# LE PHISHING

Le phishing consiste à obtenir vos coordonnées bancaires, vos identifiants de connexion ou encore vos identifiants d'accès à un réseau professionnel à l'aide d'un courriel frauduleux qui n'hésitera pas à utiliser les logos et chartes graphiques des administrations ou entreprises les plus connues.

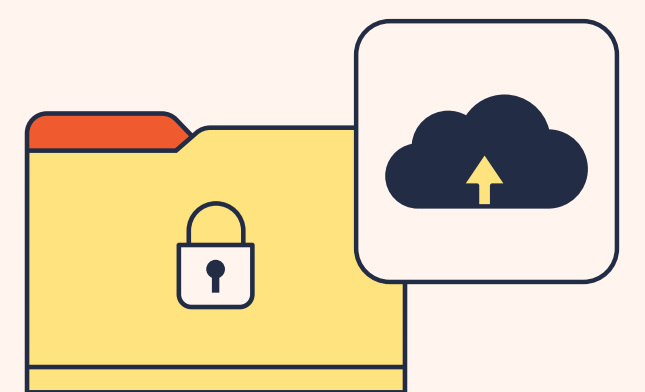
## Quels sont les risques du phishing ?

**1 Usurpation d'identité**  
Les données volées peuvent être utilisées pour usurper l'identité d'employés ou de dirigeants de l'entreprise, ce qui peut avoir des conséquences juridiques et financières graves.

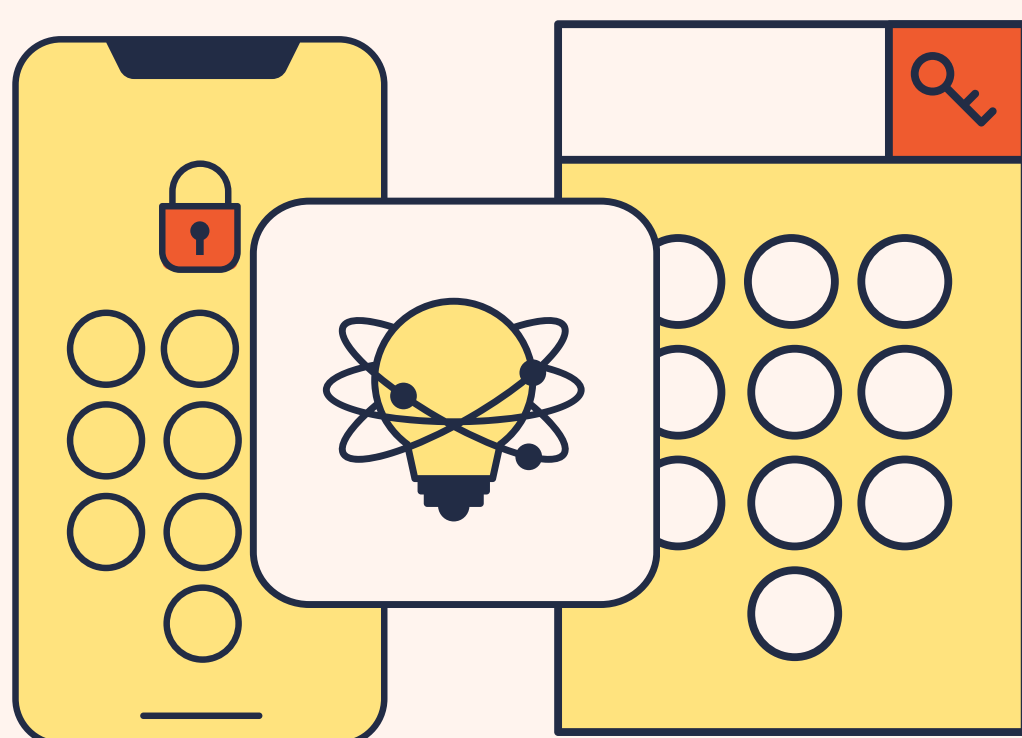
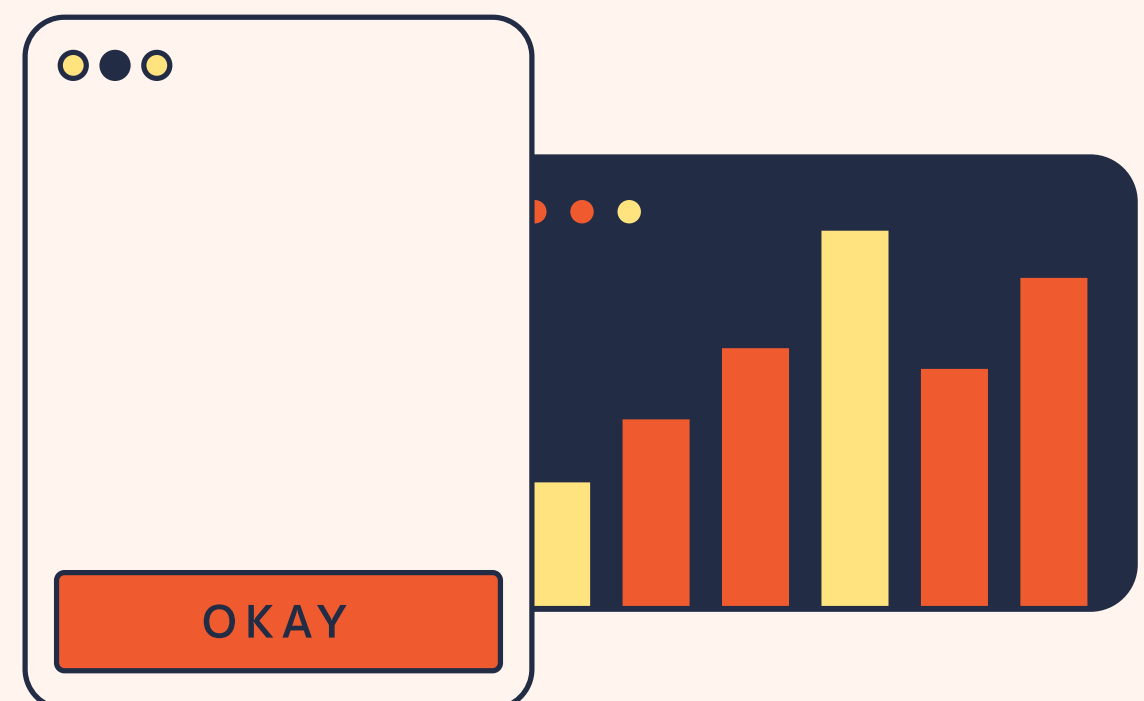
**2 Pertes financières**  
Les attaques de phishing peuvent causer d'importantes pertes financières, par exemple si des fraudeurs parviennent à accéder à des comptes bancaires ou à mener des opérations frauduleuses en utilisant les informations volées.



## Comment s'en protéger, les mesures préventives



**3 Prudence dans les emails et les liens**  
Evitez de cliquer sur des liens non fiables ou de télécharger des pièces jointes douteuses.



**4 Contact**  
En cas de doute, contactez si possible l'organisme concerné pour confirmer le message ou l'appel que vous avez reçu.

**5 Mises à jour régulières**  
Veillez à mettre à jour vos logiciels et applications pour pouvoir bénéficier des dernières fonctionnalités de sécurité.

