

# Les 4 principales cybermenaces

à connaître



## RISQUE 1 Piratage de mots de passe

1

**De quoi s'agit-il :** Les pirates exploitent des identifiants volés pour accéder à un réseau d'entreprise, obtenir des privilèges d'administrateur ou pour pirater des comptes utilisateur.



**80 %**  
des fuites de données par piratage sont liées à des mots de passe faibles ou volés<sup>1</sup>.

Le coût moyen d'une fuite de données en 2022 a atteint

**4,45 millions de dollars,**  
un record historique<sup>2</sup>.



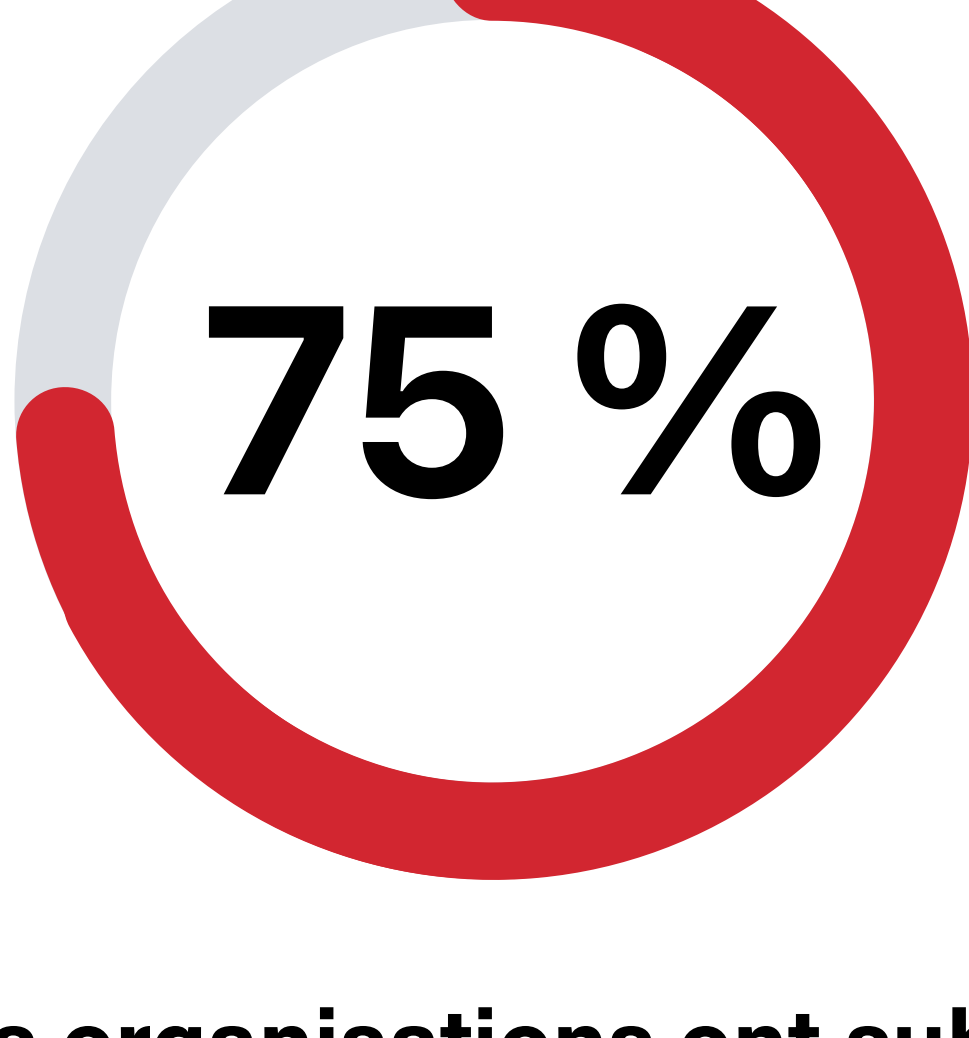
## RISQUE 2 Logiciels malveillants

2

**De quoi s'agit-il :** Logiciel nuisible installé discrètement sur un appareil pour permettre à des pirates d'accéder à des données ou des comptes.



des PME ont subi une attaque par logiciels malveillants<sup>1</sup>.



des organisations ont subi la propagation de logiciels malveillants entre employés<sup>3</sup>.

## RISQUE 3 Hameçonnage

3

**De quoi s'agit-il :** Une tentative de dérober des identifiants ou d'autres informations sensibles en incitant les utilisateurs à visiter des apps ou des sites malveillants.

**Plus de 255 millions**  
de tentatives d'hameçonnage ont été signalées en 2022<sup>1</sup>.



Les attaques par hameçonnage coûtent en moyenne

**65 343 heures**

par an aux entreprises de 10 000 employés<sup>3</sup>.

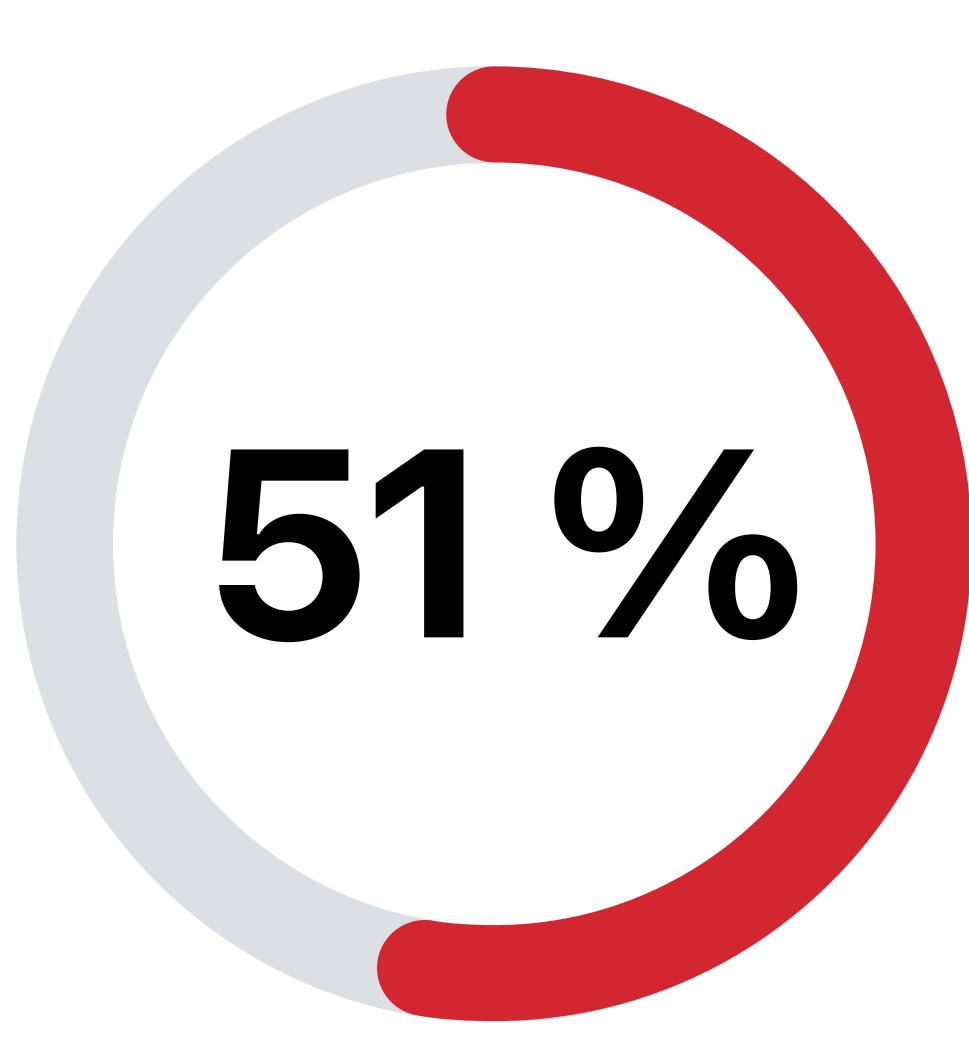
## RISQUE 4 Rançongiciels

4

**De quoi s'agit-il :** Logiciel malveillant qui vole et chiffre les données de sa cible et qui demande une rançon pour les restituer.



des PME ont subi une attaque par rançongiciel



des petites entreprises victimes de rançongiciels paient la rançon<sup>3</sup>.



**LastPass peut contribuer à bloquer les cyberattaques les plus courantes.**

**En savoir plus**

Sources :

(1) <https://www.verizon.com/business/en-gb/resources/2022-data-breachinvestigations-report-dbir.pdf>

(2) <https://www.swktech.com/costs-of-a-cyber-attack-for-smbs/>

(3) <https://www.comparitech.com/antivirus/malware-statistics-facts/>