

# Combien coûte la protection de votre identité numérique ? Moins que vous pourriez le penser.

## Tout a un coût, y compris votre identité numérique.

Comment se protéger des pirates qui œuvrent jour et nuit pour voler vos données ?

Et combien faut-il dépenser pour protéger vos informations confidentielles de leurs regards indiscrets ?



## Voici ce que valent vos informations.

Les pirates peuvent se faire un joli pactole en vendant vos données sur le « dark web »<sup>1</sup>.



## Bien que les données personnelles soient précieuses, les gens ne les protègent pas.



**seuls 50 %**

des gens estiment que leurs données sont en sécurité en ligne<sup>2</sup>, mais la plupart n'agissent pas en conséquence.



**seuls 55 %**

changeraient leur mot de passe si leur compte était piraté<sup>3</sup>.

## Les gens font passer le plaisir avant la sécurité.

Lorsqu'on leur demande ce qui les pousse à tester une nouvelle technologie :

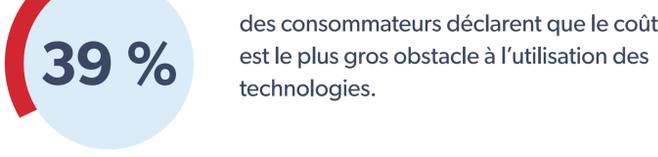


**62 %** citent le potentiel de divertissement.



**21 %** citent le renforcement de la sécurité<sup>5</sup>.

## Les gens utilisent le coût comme prétexte



## Mais les dépenses consacrées aux applications augmentent tous les ans. Alors, le coût est-il vraiment le problème ?



## Inutile de prétexter le coût.

Continuez à consacrer vos dépenses aux jeux et au divertissement, et adoptez ces 5 façons gratuites de protéger votre identité numérique.



- Protégez vos mots de passe :** créez des mots de passe uniques et robustes pour tous vos comptes, et utilisez un gestionnaire de mots de passe gratuit qui les mémorise et les saisit à votre place sur tous vos appareils.
- Configurez le suivi de votre compte :** des services de suivi gratuits vous sont proposés par votre banque et peuvent vous alerter en temps réel des mouvements bancaires sur vos comptes.
- Activez l'authentification multifactor :** la plupart de vos comptes les plus sensibles, comme votre e-mail ou votre banque offrent l'AMF gratuitement, afin de compliquer la tâche des pirates.
- Divulgez le moins possible :** les pirates utilisent les informations publiées sur les réseaux sociaux pour vous tromper par le biais d'e-mails et d'appels téléphoniques frauduleux.
- Assurez la sécurité de tous vos appareils :** actualisez le système d'exploitation, exécutez des logiciels antivirus et utilisez un gestionnaire de mots de passe qui préremplit les mots de passe sécurisés sur tous vos appareils.

**LastPass mémorise tous vos mots de passe sur tous vos appareils, gratuitement !**

[www.lastpass.com](http://www.lastpass.com)

Sources :  
1. <https://www.experian.com/blog/ask-expert/does-how-much-your-personal-information-is-selling-for-on-the-dark-web/>  
2. Données d'enquête LastPass  
3. <https://blog.lastpass.com/2018/05/psychology-of-passwords-neglect-is-helping-hackers-win.html/>  
4. <https://seniorbaker.com/blog/app-revenue-and-downloads-2019>  
5. Données d'enquête LastPass