

Cyber-attaque Boulanger : ce qu'il faut faire

Les informations volées sont celles qui avaient été mises en vente sur le dark web, ([signalé dès le 7 septembre](#)). La base de données compromise contiendrait les informations de **27 millions de clients français**.

Ce que vous devez faire maintenant

les clients de Boulanger, et plus largement tous les consommateurs français, : mesures pour se protéger :

1. Restez vigilants face au phishing : les cybercriminels pourraient utiliser vos informations personnelles pour créer des e-mails ou des SMS de phishing très convaincants. Méfiez-vous de toute communication suspecte, même si elle semble provenir de Boulanger ou d'autres entreprises légitimes.
2. Changez vos mots de passe : si vous utilisez le même mot de passe pour votre compte Boulanger et d'autres services, changez-les immédiatement. Utilisez un gestionnaire de mots de passe pour créer et stocker des mots de passe uniques et complexes pour chaque compte.
3. Activez [l'authentification à deux facteurs \(2FA\)](#) : cette mesure ajoute une couche de sécurité supplémentaire à vos comptes, même si vos identifiants sont compromis.
4. Surveillez vos relevés bancaires : bien que Boulanger affirme qu'aucune donnée bancaire n'a été compromise, restez attentifs à toute activité suspecte sur vos comptes.
5. Soyez prudents avec vos informations personnelles : limitez le partage de vos données personnelles en ligne et assurez-vous de la légitimité des sites web avant de fournir des informations.

6. Parlez-en à vos proches : ils ne sont certainement pas au courant.