okta

What's the cost of identity theft?

Our personal data is valuable to criminals. This is turbocharging the rise in account takeovers, where hackers use genuine login credentials to gain access to accounts and steal information. The impact on an organisation's revenue and reputation can be huge – so how can businesses mitigate risks and maintain trust?

Account takeovers are thriving

Account takeovers rose threefold during the pandemic, as more people shopped and worked online.

3x
Increase between 2019 and 2021
Source: Sift

User identities are under attack

Stolen or compromised credentials were the top cause of all data breaches in 2021.

61%
of data breaches in 2021 involved misused credentials
Source: Verizon DBIR

> "Hackers don't break in, they log in"
>
> Bret Arsenault, Microsoft

Criminals obtain credentials in multiple ways

Users can be deceived into revealing credentials in phishing attacks or lists of common and stolen passwords can be bought from the dark web.

7 in 10
organisations have experienced an increase in phishing attacks since the pandemic began.
Source: Sophos

15 billion
credentials are openly for sale on the dark web
Source: Dark Shadows

Weak password security is fuelling the problem

Many people use easily guessable passwords or reuse the same one across many websites, increasing their exposure to attack.

123456
Most common password in 2021
Source: NordPass

14
No. of times a password is reused on average
Source: LastPass

How do hackers get into your systems?

Credential stuffing	Password spraying	Phishing
Hackers test stolen credentials across thousands of different websites until an account gives in. This is often successful because people reuse credentials.	Hackers bombard user accounts with commonly used passwords to see if any of them work. This succeeds because people use easily guessable passwords.	Users are tricked into revealing their credentials, for example in an email inviting them to follow a link to a website

55%
of data breaches are committed by organised criminal groups
Source: Verizon DBIR

Data breaches are bad for business

Many cyber criminals use online tools to spray masses of different passwords at websites to break them.

47%
of customers would permanently stop using a brand after hearing of a data breach
Source: The State of Digital Trust, Okta

$4.2 million
Average cost of a data breach in 2021
Source: IBM Cost of a Data Breach Report

3 ways to protect customers' identities

1. Detect breaches faster

Breach detection systems such as Auth0's Credential Guard can detect breaches as soon as they happen and quickly reset affected passwords.

2. Implement multi-factor authentication

Multi-factor authentication adds an extra layer of security beyond a user's password that helps keep hackers out of your systems.

3. Go passwordless

More organisations are now choosing to do without passwords altogether, offering customers secure, user-friendly login methods like biometrics, one-time passwords and magic links.

Prevent account takeovers with Okta

Okta helps secure your customers, partners and employees with authentication solutions they can trust. Enforce strong password policies, quickly identify fraudulent login attempts and block bad actors with Okta's automated threat detection capability.

To learn more about how to stop account takeovers, watch the video podcast with Brian Glick, Computer Weekly Editor in Chief, and Okta's Ian Lowe.

© All rights reserved. Okta 2022