Arkose Labs

# The True Cost of ATOs - Are your customer accounts safe?

When a user suffers an account takeover (ATO) attack, companies might just succeed to cyber risk—they can suffer lost customers, impacted market share, and damaged brand trust. An increasing number of these attacks could demand more stringent practices and vigilance to stop ATOs before users are impacted. But, despite the threat ATOs present, many IT executives don't plan to increase their budgets for fraud prevention.

**Arkose Labs and Pulse surveyed 100 tech executives to understand:**

- The frequency of account takeovers
- How account takeovers have impacted their businesses
- How fraud budgets will shift in 2021

Data collected from Jan. 23 - Mar. 16, 2021

Respondents: 100 IT executives

## Rising account takeover attacks have come at a high cost for companies.

More than half (53%) of IT executives say they have seen an increase in account takeover attacks in the past year. Only 18% saw the number of attacks decrease.

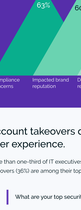
How has the frequency of account takeover attacks changed at your company over the last 12 months?


Of the technology executives who saw a surge in account takeover attacks over the past year, more than half (57%) saw an increase of more than 10%.

To what extent did the number of account takeover attacks increase in the past year?


61% of IT executives estimated that recovering compromised accounts cost their organization more than $100,000.

How much would you estimate that account takeovers cost your business in 2020?



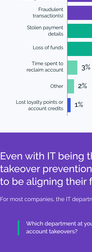

## Account takeovers led to customer loss and amplified security concerns for businesses.

Nearly half of IT executives (49%) agree that account takeovers have led to the loss of clients.

To what extent do you agree that your business has lost customers due to their accounts being hacked in the past year?


In addition to lost customers, A majority of IT executives (53%) say they faced compliance concerns following account takeovers, as well as impacted brand reputation (60%) and loss of revenue (46%).

How did account takeovers affect your business in 2020?




## Account takeovers drastically impact the user experience.

More than one-third of IT executives say fake account registrations (37%) and account takeovers (36%) are among their top security concerns regarding their business's website

What are your top security concerns for your business's website?


90% of IT executives believe that account takeovers negatively impact user experience.

To what extent would you agree that account takeover attacks impact user experience?


According to 40% of IT executives, compromised identity credentials have the most significant impact on end users, followed by fraudulent transactions (32%).

What is the most significant impact on your customer/end-user from account takeovers?


## Even with IT being the go-to department for account takeover prevention, not many organizations seem to be aligning their fraud budget in 2021.

For most companies, the IT department is responsible for preventing account takeovers (72%).

Which department at your company is tasked with preventing account takeovers?




While more than one-third (37%) of IT executives allocated more than 5% of their tech budget to fraud, almost two-thirds (60%) allocated less than 5%—and some (3%) didn't include fraud prevention in their tech budget at all.

A majority of IT executives (93%) allocated up to 10% of the IT budget for fraud prevention in 2020.

How much of your overall technology budget was allocated to preventing fraud in 2020?


And despite the growing number of account takeover attacks reported by IT executives, almost half (47%) don't plan to increase their spend on fraud prevention in 2021.

How do you anticipate your fraud budget will change in 2021?


## Respondent Breakdown

Region




Title




Company Size




Insights powered by PULSE