How Can You Spot When an Account Has Been Taken Over?
Our vision today is to build the leading risk data engine for digital profiling in emerging and high-risk economies.
Did you know?

$4 \text{ BILLION}$

of losses for businesses worldwide.

$263$

out of their own pocket to resolve an ATO.
Business damages

- Strain on your IT team
- Support is overwhelmed by customer requests
- The finance department must fight chargebacks
- Loss of reputation and brand trust
- Stocks can plummet after a publicized breach
<table>
<thead>
<tr>
<th>Category</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquiring more data</td>
<td></td>
</tr>
<tr>
<td>Financial fraud</td>
<td></td>
</tr>
<tr>
<td>Virtual currency fraud</td>
<td></td>
</tr>
<tr>
<td>Promo abuse</td>
<td></td>
</tr>
<tr>
<td>Card testing</td>
<td></td>
</tr>
<tr>
<td>Spam</td>
<td></td>
</tr>
<tr>
<td>Phishing</td>
<td></td>
</tr>
<tr>
<td>Ransom attacks</td>
<td></td>
</tr>
<tr>
<td>Account reselling</td>
<td></td>
</tr>
</tbody>
</table>

Why every account is valuable

#LoyaltyFraud Loyalty Security Association
Spring Conference 2020
Anatomy of an ATO

01
STEP

Fraudster finds an online store account credentials, either by phishing or finding them in a data breach.

02
STEP

They log in and change the shipping address.

03
STEP

The fraudster buys items with the account’s linked credit card.

04
STEP

They use the same account to resell the item on a legitimate marketplace.
Bad Agents

- Brute force
- Phishing
- Malicious software
- SIM hijacking
- Lax password protection
- Advanced phone hijacking

#LoyaltyFraud Loyalty Security Association
Spring Conference 2020
How businesses should prevent ATO’s

1. Follow the best data protection practices
2. Use SSL
3. Encrypt if possible
4. Physical device security
5. Hire white hat hackers
5. Make use of dynamic authentication
Flagging suspicious user behaviours

Unusual number of chargeback requests

Hundreds of login attempts on one account
Flagging suspicious user behaviours

- Mass password reset requests
- Shipping address changes
Flagging suspicious user behaviours

Very large purchases

Multiple changes to an account in one session
Flagging suspicious user behaviours

Transfers of a large number of reward points

Suspicious change in browser use, ISP, new country or VPN use
Flagging suspicious user behaviours

- Multiple customers using the same IP or device
- Use of emulators, virtual machines
Dynamic Authentication

User login

Fraud check passed?

Apply further verification

MFA passed?

Login confirmed

Decline

Allow checkout

Successful transaction
How can account takeovers be stopped?

UX
Seamless payment

Security
Preventing account takeovers
Thank you
for your attention

Bence Jendruszátk
bence@seon.io