Account sharing and turnover: Turning loss to loyalty

Diane Benjuya, IBM Security
Gregor Frimodt-Moeller, Group CEO, any.cloud
$9.1 Billion, 2019

$12.5 Billion, 2024

Park Associates 2020
“Credential sharing falls into two categories. Most sharing is casual, with no intent to profit.”

“But the bigger risk is from pirates that purchase large stolen consumer databases via the 'Dark Web' and use automation to discover penetrable end user accounts.”
Digital identity fraud “kill chain”

1. Compromised account
2. Fraudulent login
3. Monitoring
4. Monetization

Malware  Phishing  Bots
Data is a steal on the dark web

Accounts of every major streaming service available - and at “great” discounts
There are many ways to clamp down on account sharing

- Manage a device list per account
- Send a security notification
- Offer an upgrade
- Block concurrent logins
- Shut down the account
Assessing digital identity risk is at the heart of the solution

- **Real time assessment of risk of fraud** of every user session
- **A frictionless experience** for low risk sessions
“We are now in a position where we are one step ahead of the hackers.”

CEO, leading European video streaming service
What is any.cloud?

- Consumer security specialist
- ISO27001 certified company
- Customers in 29 countries
- CSA Star Alliance certified
- IBM’s most innovative partner in Europe, 2020
- IBM Cloud Partner of the Year 2017 and 2019 in Denmark
- Headquarters in Copenhagen and offices in Poland, the Czech Republic and Finland
- Founded in 1998
Your password is incorrect
Reenter password
Login
Warning!
Please, update your user
SEND VERIFICATION CODE
Your account has been hacked
two-factor authentication
Select all images
Click here to agree
Your password is incorrect
Someone logged into your account
Warning!
Please, download!
Keep Your Privacy Settings On
Warning!
Your account has been hacked
two-factor authentication
Select all images
Click here to agree
World population 2020: 7.8 billion

Users online 2020: 4.5 billion

Source: World Statista, 2020
Our ideology

Customer Experience

Digital Trust

Fraud Prevention
How does account profiling work?

Think about if you were to secure the journey without impacting the online experience for the user.
Securing who is who

Pinpoint data to be consumed by the application or third party risk engine

**Device Intelligence**
- Device ID
- Screen Resolution
- Screen dpi
- Screen touch
- Client time zone
- First seen/last seen
- Last change
- Rapport_machine_id
- OS languages
- Platform/CPU/OS
- User Agent
- Random cookie
- Blacklisted/ KnownFraudster
- RAT Indication
- Proxy indication
- Spoofed device

**Connection/Analytics**
- Remote Addr
- IP class
- ISP
- Org
- Country
- Region
- City
- Post code
- IP time zone
- Longitude-Latitude
- Referrer
- x_forwarded_for
- Network IPs path
- Area Code
- Accepted content types

**Browser Intelligence**
- activeX
- history_length
- js_enabled
- accept_encoding
- Counter
- Digest
- Fonts
- file_upload_indicator
- Mimes
- file_upload
- navigator_props
- browser_version
- client_charset
- Browsers + version
- Character set
- Languages
- network_data
- plugins

**Passive Biometrics**
Blacklisted/ Known Fraudster based on:

**Keyboard Input**
- Input normal
- Input bad
- Input anomaly
- Input Scripted
- Input replay
- Input automation

**Mouse Input**
- Mouse type
- Mouse bad
- Mouse anomaly
- Mouse replay
- Mouse automation

**Threat Intelligence**

**Malware Data**
- Malware ID
- Malware Name
- Organization is Targeted

**Carrier Analytics**
- Phone type
- Name match
- Address match
- Contract type

**Risk Assessment**
- Risk Score
- Risk Reason: RAT, SE, new device after phishing, etc.
- Recommendation
Over 50B web hits per month

Over 300 TB data

<516 billion data events
500K malware samples
140K phishing sites
120K malware configurations
3K security updates
Business case

BLOCKBUSTER®
So... how can we elevate your platform?
Win-win: Identity risk protection meets a differentiating customer experience
Thank you

Contact us:

**Patrick Vowles, IBM, Americas**
patrick.vowles1@us.ibm.com
ibm.com/security

**Diane Benjuya, IBM Worldwide**
diane@il.ibm.com
ibm.com/security/fraud-protection/trusteer

**Gregor Frimodt-Moeller, any.cloud**
gm@anyccloud.dk
linkedin.com/in/gregormoller
https://retrust.global

When you interact with IBM, this serves as your authorization to MESA or its vendor to provide your contact information to IBM in order for IBM to follow up on your interaction. IBM’s use of your contact information is governed by the IBM Privacy Policy.