Is cyber security getting under your company skin?

How to fight online frauds with smoothest UX

Michal Antoniak
Cyber Security Consulting Manager

Joint Fraud Conference
The Chinese Wall syndrome
The Chinese Wall syndrom
Why the old concept backfires?

„The more secure you make something, the less secure it becomes.”

Don Norman
jnd.org
More Security ≠ Less Friction

99% IT departments believed 2FA was the best way to protect an identity and the access to it

74% admit that they receive complaints about it from their users

https://betanews.com/2017/01/11/2fa-complaints-rise/

Joint Fraud Conference
When the friction is just too much

Too complex password policies

Too many Authentication factors

Joint Fraud Conference
The Human Factor

Accidents in Aviation

- Human Causes: 80%
- Technical Causes: Remaining 20%

1903 - present

Joint Fraud Conference
The Human Factor

95% of all successful cyber attacks is caused by human error

Source: IBM Cyber Security Intelligence Index
The Human Factor

In 2018 and 2019, the combined threats of phishing and credential stuffing made up roughly half of all publicly disclosed breaches in the United States.
More Security & Less Friction?

Adaptive Authentication

Passwordless MFA

AI/ML Analytics

Continuous adaptive trust (CAT)

Joint Fraud Conference
Passwordless MFA – better UX

NOW

• Phone-as-a-token and mobile MFA

Comming SOON

• FIDO2
### Adaptive Authentication – more Security

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Credential Stuffing (ATO)</strong></td>
<td>- Device recognition – identifying changes in device unique fingerprint</td>
</tr>
<tr>
<td></td>
<td>- Geolocation feature – comparing users geolocation from GPS with the one from IP address</td>
</tr>
<tr>
<td></td>
<td>- Behavioral biometrics – distinguishing between man and machine and verifying typical user activities</td>
</tr>
<tr>
<td><strong>Malware Infection</strong></td>
<td>- Malware detection (even if it was installed during users session)</td>
</tr>
<tr>
<td></td>
<td>- Untrusted sources application detection</td>
</tr>
<tr>
<td></td>
<td>- Root or jailbreak mode detection</td>
</tr>
<tr>
<td></td>
<td>- Webpage integrity check</td>
</tr>
<tr>
<td><strong>Identity Clonning</strong></td>
<td>- Detecting cloned email addresses</td>
</tr>
</tbody>
</table>
Adaptive Authentication - more Security & better UX

- Recognition
- Risk Signals
- Access Risk Signals
- Risk Scoring Engine

Joint Fraud Conference
Adaptive Authentication - more Security & better UX

Recognition & Risk Signals

- Device recognition
- Malware detection
- Anti-Tamper
- Behavioral biometrics
- Geolocation
- Identity cloning protection

Access Risk Signals

- Security Policy

Risk Scoring Engine
Adaptive Authentication - more Security & better UX

Risk Scoring Engine

- Device recognition
- Malware detection
- Anti-Tamper
- Behavioral biometrics
- Geolocation
- Identity cloning protection

Recognition & Risk Signals

Access Risk Signals

MFA

Security Policy

Joint Fraud Conference
Adaptive Authentication - more Security & better UX

Recognition & Risk Signals
- Device recognition
- Malware detection
- Anti-Tamper
- Behavioral biometrics
- Geolocation
- Identity cloning protection

Access Risk Signals
- Security Policy

Risk Scoring Engine

Deny

Joint Fraud Conference
Adaptive Authentication - more Security & better UX

- Recognition
- Risk Signals
- Identity Proofing
- Access Risk Signals
- Anti-Fraud
- Risk Scoring Engine
- BYOI
- KYC

Joint Fraud Conference
Continuous Adaptive Trust concept
Continuous Adaptive Trust concept

- Recognition & Risk Signals
  - Device recognition
  - Malware detection
  - Anti-Tamper
  - Behavioral biometrics
  - Geolocation
  - Identity cloning protection

- Access Risk Signals
  - Security Policy
  - Anti-Fraud

- Risk Scoring Engine

- AI Decision Engine

- MFA
- Identity Proofing
- BYOI

Joint Fraud Conference
Continuous Adaptive Trust concept

Joint Fraud Conference

Recognition & Risk Signals
- Device recognition
- Malware detection
- Anti-Tamper
- Behavioral biometrics
- Identity cloning protection

Access Risk Signals
- Security Policy
- Anti-Fraud

Risk Scoring Engine
AI Decision Engine

MFA
Identity Proofing
BYOI

Allow

Events

KYC

COMARCH

LSA
LOYALTY SECURITY ALLIANCE
CONCEPT change

- Protects, but is not visible
- Does not impair your UX

Joint Fraud Conference