Protecting customers from themselves

As social engineering scams proliferate, financial institutions must adopt new strategies to combat fraud and maintain trust.

BY JOHN PAUL BLAHO

Social engineering scams around the world are growing in number. Most of these scams are carried out over the phone, with losses to American consumers estimated at nearly $30 billion. A significant percentage of account takeover incidents involved some form of social engineering voice scam. According to the Federal Trade Commission, impostor scams were the number one type of fraud reported by consumers in 2020.

Financial institutions have been struggling for years to address the challenge of social engineering scams. What makes these scams hard to detect is that the cybercriminal does not interact directly with the banking platform, but, rather, persuades victims to execute payments themselves. In such cases, authentication controls based on a device, IP or location will appear genuine. Even when risk is detected and step-up authentication is required, such as out-of-band SMS one-time password, the authentication is successful because a legitimate user is performing the transaction.

Fraud prevention solutions built on device elements and network data points are no longer a match for cybercriminals who have learned to easily spoof them. Deeper visibility into risk, including behaviors associated with each step of the digital banking journey, is required.

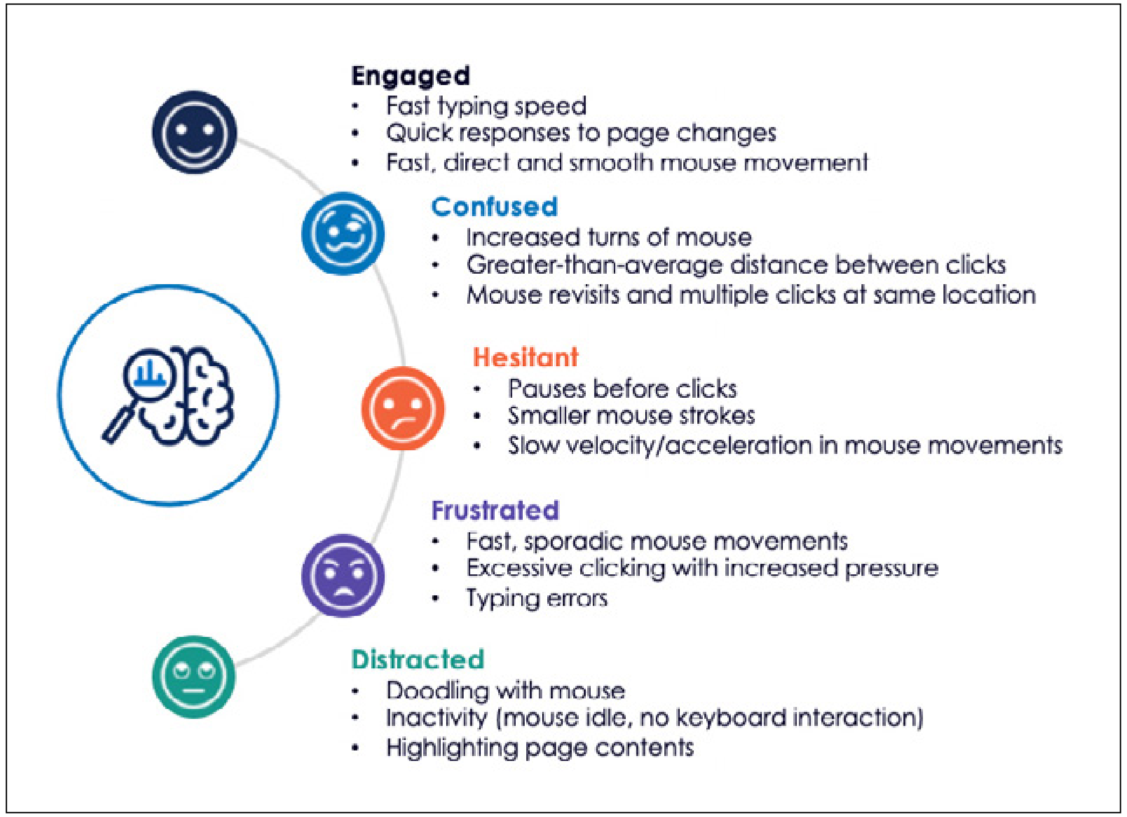
EVERY SWIPE TELLS A STORY

Behavioral biometrics plays a crucial role in helping financial institutions identify and stop social engineering scams.

Even when a genuine user is making the payment, subtle changes in digital behavior when acting under the influence of a cybercriminal can suggest a social engineering scam may be at play. Behavioral insights obtained from data collected can help build a picture of a user's typical online habits to help financial institutions detect unusual behavior when the user is reacting to a challenge or a demand during a digital session.

The illustration below summarizes a few of the behaviors a victim of social engineering may exhibit during a session and how these can be interpreted.

Each individual behavior on its own does not imply social engineering. When combined with hundreds of other behavioral, device and network data points and compared against the norms of the genuine population, these insights have the potential to illustrate a fraudulent transaction or session.



Engaged
- Fast typing speed
- Quick responses to page changes
- Fast, direct and smooth mouse movement

Confused
- Increased turns of mouse
- Greater-than-average distance between clicks
- Mouse revisits and multiple clicks at same location

Hesitant
- Pauses before clicks
- Smaller mouse strokes
- Slow velocity/acceleration in mouse movements

Frustrated
- Fast, sporadic mouse movements
- Excessive clicking with increased pressure
- Typing errors

Distracted
- Doodling with mouse
- Inactivity (mouse idle, no keyboard interaction)
- Highlighting page contents

> **Behavioral insights obtained from data collected can help build a picture of a user's typical online habits to help financial institutions detect unusual behavior when the user is reacting to a challenge or a demand during a digital session.**

Consider something as simple as a customer who is on an active phone call while navigating a live session in a mobile banking app. The indicators for this activity are significantly different than what historical data analysis would suggest is genuine behavior:

- *Fewer than 1% of all Android users combine phone calls with mobile banking activity.*
- *More than one in four confirmed cases of fraud show that the victim was on an active phone call.*
- *Data shows that an active call is 30 times more prevalent in the fraud population than the genuine population.*

In light of these differences, an active call during a live banking session can be used with other data points as a strong indicator of social engineering.

HOW TO SPOT SOCIAL ENGINEERING SCAMS

Adopting a strategy to address the rise in social engineering scams—and to identify "authorized" payments that really aren't authorized at all—should focus on four primary areas.

Customer protection across all account types: Current data shows that cybercriminals are targeting more victims with lower values, rather than the very targeted, high-value cases they used to focus on. For example, roughly a third of impersonation

scam cases in 2020 involved amounts exceeding $1,000, but this year, only about one in five cases involves values running into four digits. All customers, regardless of their financial investment within your organization, are at risk.

Education to create an informed customer: Government regulation and industry initiatives provide incentives for financial institutions to rethink their consumer education programs. Besides avoiding financial losses and the impact on reputational risk, financial institutions can use investment in consumer awareness as a brand differentiator.

Cross-channel protection: Mobile applications are becoming increasingly popular among customers and cybercriminals alike. Upwards of 70% of social engineering scams now involve mobile devices. With more customers adopting mobile banking applications for their financial transactions, social engineering scam detection should thus be weighted toward the preferred digital platform.

> Upwards of 70% of social engineering scams now involve mobile devices. With more customers adopting mobile banking applications for their financial transactions, social engineering scam detection should thus be weighted toward the preferred digital platform.

Incorporate behavioral biometrics: With social engineering scams playing a larger role in account takeover fraud, implementing behavioral biometrics can provide visibility beyond device and network data points, improve your ability to identify high-risk transactions and significantly reduce fraud.

John Paul "JP" Blaho is senior director, product marketing at BioCatch.