NICE · ACTIMIZE

Stay Ahead of Fraud

Same Fraud Schemes, With a COVID-19 Twist

The fraud threat landscape is constantly shifting – and in times like these, fraudsters find new ways to attack and take advantage of people under stress who are more likely to fall victim to scams.

Staying Ahead: Identifying New Flavors of Fraud Schemes

Agility is key as financial services organizations address the inevitable. Best practices, like applying consortium-based analytics in real time, will help detect these known social engineering scams.

Spoofing Government and Healthcare Organizations → **"Phishing", "Smishing", and "Vishing"**

Fraudsters are impersonating health agencies to carry out social engineering scams, including fake donation requests, email spoofing and fraudulent phone calls.

Fake Websites → **Malware and Account Takeover Scams**

Criminals are taking advantage of global fear by creating fake websites promising vaccines, testing kits and cures for COVID-19. Be wary of websites that request money in exchange for on-demand items. Websites also open the opportunity to infect devices with malware.

Seller and Buyer Scams → **Instant P2P Payment Scams**

Fraudsters are "selling" in-demand goods through instant P2P payment scams on avenues like Zelle.

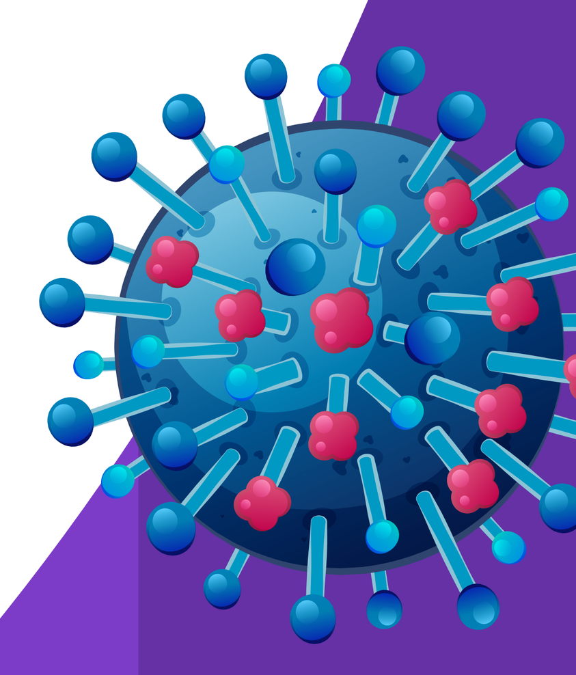
Social Media Scams → **Elder Abuse or Investment Scams**

Social media can provide convincing charity cases or investment schemes, especially those targeting the elderly.

Misinformation → **Impulsive Victims**

By spreading fear and misinformation, fraudsters are making it easy for a nervous public to fall for their scams.[1,2]

Following best practices for fraud management always holds true, even in times of uncertainty.



Anticipating the Inevitable Changes in Behavior: Customer or Fraudster?

Expect to see an increase in web and mobile banking registrations, as well as increased use of P2P services – as families, friends and neighbors assist each other while self-isolating.

Is that 70+ elderly customer genuinely enrolling in online banking?

Remember to examine your customers' behavior with a holistic view. Use a real-time fraud management solution to score customer enrollments, logins and opt for two-factor authentication.

With an agile system in place, organizations can quickly change rules or update models as they work to protect their customers.

NICE Actimize Fraud Management & Authentication solutions can help you stay ahead of evolving threats.

Learn More >

1. Glassberg, J. (2020, March 8). Coronavirus: 6 scams to watch out for. Retrieved March 18, 2020, from https://finance.yahoo.com/news/coronavirus-scams-to-watch-out-for-182236936.html

2. COVID-19 Fraud. (2020, March 23). Retrieved March 23, 2020, from https://www.justice.gov/usao-wdva/covid-19-fraud

info@niceactimize.com | www.niceactimize.com/blog | @nice_actimize | linkedin.com/company/actimize | facebook.com/NICEActimize