SEI New ways. New answers.®

4 Emerging Fraud Threats

Experts are warning businesses and computer users to beware of 2021's emerging cyber-threats.

1. **Synthetic identity fraud.** This type of fraud, which occurs when crooks use a combination of real and fake information to create an entirely new identity, is the fastest growing type of financial crime. In 2021, criminals are expected to use fake faces for biometric verification. These "Frankenstein faces" will use artificial intelligence to combine facial characteristics from different people to form a new identity, creating new security challenges.

2. **Bogus COVID "solutions."** With the distribution of vaccines underway and wider availability of rapid COVID-19 testing, fraudsters will continue to find opportunities to capitalize on anxious and vulnerable consumers and businesses. It's important to be vigilant against bad guys using the promise of at-home test kits, vaccines, and treatments as lures for sophisticated phishing attacks, telemarketing fraud, and social engineering schemes.

3. **Stimulus fraud (again).** For Americans suddenly out of work or struggling with the financial fallout from the pandemic, 2020's government-issued stimulus funds were a welcome relief, but also an easy target for fraudsters. Criminals will take advantage of additional stimulus funding by using stolen data from consumers to intercept stimulus or unemployment payments.

4. **Constant automated attacks.** Once the stimulus fraud attacks run their course, analysts predict that hackers will increasingly turn to automated attacks, including script creation (using fraudulent information to automate account creation) and "credential stuffing" (using stolen data from a breach to take over a user's other accounts) to make cyberattacks and account takeovers easier and more scalable than ever before. With billions of records exposed in the U.S. due to data breaches annually, this type of fraud will prosper in 2021 and beyond.