

# Fraud Simulation Test Your Readiness!

The purpose of cyber fraud simulations is to identify and maximize Financial Institution's (FI) immunity for fraud attacks. Each institution operates according to its own rules, size and state regulations and offers its customers different service offering. In addition, each institution treats its systems & security with different levels of hardening.

**For these reasons, fraud testing and simulations must cover all channels to include:**



### Mortgage Fraud Simulation

The purpose of this simulated attack is to understand the FI's system for detecting malicious actors trying to manipulate mortgage request procedures.



### Debit Card Fraud Simulation Testing

Understand the flaws in your fraud detection software and act accordingly in order to enhance its efficiency and protect your customers.



### Deposit Fraud Simulation Testing

The purpose of these tests is to identify fake deposit scenarios that bypass the detection system and upgrade its configuration accordingly in order to avoid real-life deposit fraud.



### Phishing Attack Simulation Testing

This simulation is designed to validate the effectiveness of your detection system and response team when phishing attacks attempt to obtain users' credentials for various fraudulent activities.



### Business Logic Manipulation Testing

Business logic testing examines the immunity of the FI's procedures to sophisticated manipulate actions performed by advanced fraudsters who know and understand the FI and its procedures.



### Physical Branch Office & Call Center Fraud Testing (Vishing)

Manipulation of the FI's employees to disclose personal information or perform illegal with draws. These attacks may include fax money transfers, SWIFT procedures and more.



### Application & Infrastructure Penetration Testing

Standard penetration tests are recommended to ensure that all applications (both internal and external), as well as the networks and servers in use, are not exposed to any attacks.



### Employee Embezzlement Simulation Testing

This kind of simulated attacks examine the integrity of the FI's employees, and are performed by elite professionals that specialize in human intelligence.

## Our Team

Our team of experts provides a leading edge in the cyber practice. They are certified and experienced professionals with diverse backgrounds in offensive & defense intelligence, network security, information technology, and cybersecurity solutions.

**Cybrella's Fraud Simulation team** experienced in fraud testing and simulations to identify Fraud and AML threats and maximize Financial Institution's (FI) immunity against fraud attacks.

## About Cybrella

Cybrella is a world leader cybersecurity consulting company HQ in Boston with an office in Tel-Aviv, Israel. Cybrella provides consulting services for all aspects of modern cybersecurity requirements – Risk Management, Frauds & AML, Cloud Security, Technology, etc. Cybrella's consulting services are aimed at providing our clients with a multi-leveled information security analysis in the following areas:

- **Cybersecurity Management** - Cyber Readiness and Strategic consulting
- **Risk Management and Application Security** - SDL (Secure Development Lifecycle) Methodology, Penetration Tests, Application Firewall, Security Awareness Training
- **Infrastructure Security and Cloud Security** - Risk Analysis and High-Level Engineering, Forensics & Incident Analysis
- **GRC** (Governance, risk management, and compliance) - Accreditation preparation for compliance with standards and regulations, writing policies and regulations
- **CISO as a Service** Cybersecurity Strategy & Management, Managed Detection & Response, Cloud Security, Cyber Readiness Road Map Development, Security Gap Analysis, Policy Review and Development, etc.

For more information Contact us  
at [boston@cybrella.io](mailto:boston@cybrella.io) or call +1.617.454.1332

Contact us