DFCC Bank: Why trust has become the new Cybersecurity battleground



Kushan Jayasuriya, Senior Vice President – Integrated Risk Management/Chief Risk Officer, DFCC Bank.

There was a time when online fraud was so obvious it hardly needed an announcement. Emails arrived with awkward grammar and improbable promises. Unknown callers spoke of lottery winnings or inheritance funds from distant countries. Fake websites looked visibly counterfeit, assembled with just enough

effort to deceive the careless, but rarely enough to fool the cautious. Back then, the boundary between legitimate communication and fraud, though imperfect, was still visible to most people. That boundary now appears to be disappearing at a frightening pace.

Today’s scams are no longer built on obvious deception. They are built on familiarity. They arrive disguised as trusted institutions, delivery notifications, investment opportunities, customer service requests, or urgent financial alerts. They mirror real brands with alarming precision and increasingly rely on behavioral manipulation rather than technical intrusion. In many ways, this marks a fundamental shift in the nature of cybercrime.

The modern scam does not force its way into systems. It convinces people to open the door themselves, much like inviting a trusted visitor into their home. That changes cybersecurity entirely.

For years, conversations about digital security focused primarily on infrastructure. Firewalls, antivirus systems, encryption protocols, authentication layers, and monitoring tools became the defining architecture of cyber defense. These remain critically important. Yet the fraud landscape has evolved faster than the public’s understanding of how cyber risk now operates.

Today, many attacks succeed not because systems fail, but because human judgment is deliberately targeted. Scammers understand urgency, Distraction, fear, authority, loneliness, and trust. Increasingly, fraud is engineered not to “hack” technology first, but to manipulate behavior and emotions. A message claiming your account is at risk. A phone call requesting urgent verification.

A payment request tied to a time-sensitive opportunity. These are not isolated tactics. They are psychological triggers meant to override hesitation. This is why awareness alone is no longer enough. People already know scams exist. What they are often unprepared for is how convincing, contextual, and emotionally persuasive modern scams have become. What makes the current environment even more concerning is the growing industrialization of fraud. Behind many scams now lies an organized digital economy operating at scale in the shadows.

One of the most significant enablers of this shift is the dark web, a hidden marketplace where cybercriminal activity is bought, sold, refined, and distributed with increasing sophistication. Stolen personal data, banking credentials, phishing

kits, malicious software, scam templates, and impersonation tools are traded with disturbing efficiency. In many cases, “fraud-as-a-service” models now enable individuals with limited technical expertise to launch highly convincing attacks by leveraging infrastructure developed by organized cybercriminal networks. The barrier to entry has collapsed. Scams that once required advanced technical expertise can now be carried out with purchased toolkits, stolen databases, and automated systems built for scale. For customers, this fundamentally changes the nature of risk.

Fraud is no longer isolated or opportunistic. It is adaptive, coordinated, and increasingly professionalized. As this environment evolves, so must the role of financial institutions. Banks today are no longer simply custodians of money.

Increasingly, they are custodians of digital trust. This shift has reinforced the importance of approaching digital trust at DFCC Bank as both a technological and behavioral challenge.

Across the banking sector, institutions are expanding cybersecurity frameworks beyond internal systems and infrastructure. Increasingly, the focus includes the wider digital environment in which customers operate. Modern banks now monitor fake websites, phishing pages, impersonation accounts, and misuse of brand identity across digital platforms.

External attack surfaces are continuously scanned to identify vulnerabilities before they can be exploited. Dark web monitoring has also become increasingly important, with financial institutions monitoring underground marketplaces and cybercriminal forums for leaked credentials, compromised customer information, and indicators of planned attack campaigns. These systems matter. They strengthen institutional preparedness and improve response capability. They help institutions move faster than threats. Yet despite increasingly advanced safeguards, one reality remains unavoidable: technology alone cannot fully solve a behavioral problem. The most effective cybersecurity control is often not technological but behavioral.

Simple habits continue to make a significant difference – pausing before responding to urgent requests, independently verifying communications, refusing to share passwords or OTPs, carefully checking URLs, and avoiding unofficial applications or suspicious links. These actions may seem basic, but they directly disrupt the psychological mechanics that most scams rely on. This is why digital hygiene is

becoming increasingly important. Much like physical safety depends on routine habits, digital safety now depends on behavioral discipline practiced consistently over time.

In practice, this requires a shift away from instinctive speed and toward deliberate verification. That shift matters because speed has become a defining characteristic of the digital economy. Payments happen instantly. Communication is immediate. Decisions are made in seconds. Fraudsters deliberately exploit this environment. Urgency remains one of the most effective tools in digital fraud because it suppresses reflection. The faster people react, the less likely they are to verify. Which is why one of the most important cybersecurity responses today is surprisingly simple: slow down. Pause before clicking. Pause before approving. Pause before responding. In many cases, the difference between a secure interaction and a compromised one is not technical expertise but a few extra seconds of judgment.

The future of cybersecurity cannot rest entirely with institutions or with customers. It must increasingly be a shared discipline.

Financial institutions must continue to strengthen systems, improve fraud detection, enhance authentication mechanisms, and invest in awareness. Customers, meanwhile, must recognize that digital judgment is now part of everyday financial responsibility. This matters because the threat landscape will continue to evolve. Artificial intelligence will likely make impersonation more convincing. Fraud attempts will become more personalized. Emotional manipulation will increasingly merge with technical sophistication. The question is no longer whether fraud will evolve. It will evolve.

The more important question is whether awareness, behavior, and institutional safeguards can evolve more quickly.

Digital banking has transformed access, convenience, and financial inclusion in remarkable ways. That progress should not be feared or reversed. But trust in digital systems cannot be sustained by technology alone. It requires awareness. It requires vigilance. And increasingly, it requires verification as a matter of instinct. In a world where scams are designed to feel believable, trust itself has become part of cybersecurity. Protecting that trust may become one of the defining responsibilities of modern banking.