USAID
FROM THE AMERICAN PEOPLE

Cybersecurity
DIGITAL FINANCIAL SERVICES

Photo credit: Hanz Rippe/Paramo Films for USAID

Why Does Cybersecurity Matter for DFS?

Digital financial services (DFS) in lower and middle income countries (LMICs) are growing both organically and through USAID assistance and take a few different forms. Public mobile money systems are increasingly popular, in some cases comprising a majority of all transactions. The mobile money platform M-Pesa in Kenya handles as much as 72% of all financial transactions across the country. USAID also uses DFS in its programming, such as with the Vietnam Forests and Deltas activity. (See the box below.) Where populations have access to digital platforms, humanitarian aid organizations use DFS to deliver aid during crises and conflict. DFS has revolutionized financial inclusion, improving access to financial services and helping to build sustainable economic infrastructure that benefits the most vulnerable individuals. But these new platforms and services are not without risks. As more data and money move through these systems, they have become highly attractive targets for cyber attacks. Digital financial systems rely on consumer confidence, and thus adequate cybersecurity protections are critical to the continued growth of the DFS sector.

What is cybersecurity, and why does it matter for international development?

As noted in USAID's Cybersecurity Primer, USAID defines cybersecurity as "the activity or process, ability or capability, or state whereby information and communications systems that support or affect development outcomes, and the information contained therein, are protected from and/or defended against damage, unauthorized use or modification, or exploitation." As USAID partner countries further their digital transformation and continue to adopt new digital tools and systems, cyber risks and vulnerabilities proliferate. Cybersecurity failures pose material threats to USAID partner countries and undermine partner country government legitimacy, USAID must protect its digital investments by ensuring that its digital programming addresses cyber harms and includes cybersecurity mitigation measures.

Vietnam Forests and Deltas

USAID's Vietnam Forests and Deltas activity worked with local community members to provide training on using mobile money to receive payments from the Government of Vietnam. Many participants already owned and were comfortable using mobile phones, but they were concerned about the safety and utility of mobile money. The training addressed misconceptions around DFS, while demonstrating its benefits, like the speed and transparency of mobile payments over cash payments.

Cybersecurity Trends in DFS

DFS-related cybercrime and cyber attacks have been rapidly increasing, even prior to COVID-19. This issue is particularly important in many USAID partner countries because many have leapfrogged over more traditional banking systems to DFS. The rapid proliferation of DFS providers increases the interconnectedness of the financial system, which, in turn, creates more opportunities for cybercrime. A senior African government official shared that in her country banking and financial services systems are under continual and increasing cyber attacks. While this has not been publicly reported out of fear of losing popular confidence, it is a major problem her country currently has insufficient capacity to address. Officials in other countries have confirmed similar high levels of cyber threat. Compounding the challenge is that most countries do not have enough trained cyber professionals in the workforce and it is difficult for governments to hire those who do exist, as they can earn much higher salaries in the private sector.

Financial sector cyber attacks doubled in Africa in 2017; the DFS sector was hit especially hard. COVID-19 only exacerbated this issue. Not only did it accelerate the public's demand for DFS, but it also accelerated the supply: over 200 countries expanded their social safety nets in 2020 and 2021, many of which used DFS to transfer the funds to individual citizens.

DFS cyber attacks affect DFS providers *and* DFS consumers. DFS providers such as mobile money services and digital loan companies are prime targets for cybercriminals because they are flush with cash and customer data. DFS providers' computer systems are subject to regular cyberattacks, such as denial of service attacks—which seek to overwhelm computer systems with a barrage of automated requests—and individual DFS employees can be targeted with social engineering or spear phishing attacks, or even with direct threats to them and their families, to access their employers' systems. DFS providers also face the risk of insider threats, where employees leverage their access to systems to commit fraud or embezzlement. Cyber criminals are also exploiting linkages within the DFS ecosystem to commit cybercrimes, such as targeting point-of-sale systems to steal consumer credit card information. While DFS providers have traditionally been the targets of cybercrime, hackers and criminal syndicates are increasingly turning to DFS consumers, who are easier targets because they often have fewer defenses against and less knowledge of cyber threats. According to research by Innovations for Poverty Action, more than 50% of Kenyan DFS users, one-third of Ugandan users, and more than one quarter of Nigerian users have experienced phishing attempts. Nearly 30% of Bangladeshi DFS users report encountering some kind of scam.


Usman Ghani for USAID

In addition to social engineering and spear phishing attacks (similar to those used on DFS provider employees) to gain access to personal accounts, cybercriminals are also creating their own predatory and fraudulent mobile financial apps to scam consumers. From 2016 to 2020, legitimate transactions conducted via mobile apps increased 34 percent, while fraudulent transactions via mobile apps increased 104 percent.

DFS cybercrime perpetrators can range from individual hackers to nation-states. The proliferation of malware-as-a-service (i.e., malware on-demand) and other evolutions in cybercrime has made it easier for individuals to launch attacks that can cripple DFS systems. One hacker took Liberia's Lonestar Cell MTN mobile network operator offline for several days in October 2016, halting mobile money transactions on its network. Because the potential financial gains are so large, criminal organizations and syndicates are also targeting the DFS sector. The Carbanak group stole around $1 billion from financial institutions from 2013-2018 by targeting employees at more than 100 banks with fraudulent emails that downloaded malware onto their targets' systems when clicked. Nation-states are also responsible for a significant number of attacks on DFS providers. State-sponsored hackers from North Korea have allegedly stolen USD $1.3 billion from financial institutions and cryptocurrency providers in countries like Vietnam, Bangladesh, and Mexico by sending fake messages that appeared to come from SWIFT (Society for Worldwide Interbank Financial Telecommunication).

DFS-related cybercrime can also be relatively low-tech. For example, business email compromise (BEC) attacks use hijacked email accounts to persuade victims to transfer money to accounts controlled by hackers.

USAID partner countries, donors, and industry leaders are promoting increased cybersecurity measures among DFS providers. Given the prevalence of fraud and cybercrime within the DFS sector, donors, national governments, and DFS providers are coming together to address the issue. The Central Bank-led Nigeria Electronic Fraud Forum is bringing together key stakeholders to combat fraud and cybercrime. Donors such as the International Monetary Fund, World Bank, and Inter-American Development Bank are focusing primarily on building the cybersecurity capacity of DFS providers and other key DFS stakeholders, as well as on bringing together the public and private sectors to determine a common set of cybersecurity standards for DFS. The International Telecommunications Union-hosted DFS Security Lab "support[s] government and industry in assessing compliance with established best practices in DFS security, establishing a security baseline for DFS applications, and adopting interoperable authentication technologies." Similarly, the Carnegie Endowment for International Peace and Accion (with funding from the Mastercard Center for Inclusive Growth) have each authored toolkits to build the cyber resilience of financial institutions and DFS providers. GSMA released a cybersecurity governance framework for mobile money providers that holistically breaks down cybersecurity across three .

Digital payments can greatly benefit development and humanitarian assistance programs, but carry risks that USAID and other donors must mitigate. In addition to supporting DFS institutions, USAID and other donors are increasingly incorporating digital payment solutions into development and humanitarian assistance activities. Cash transfers can greatly benefit program participants, especially when coupled with training and other interventions. However, these programs can bring a bevy of new risks when cash is transferred and held digitally. USAID and other donors must ensure that these cash transfer programs do not put already vulnerable people at risk by exposing their data and funds to governments, companies, and cyber criminals. All digital cash transfer activities that are incorporated into development and humanitarian assistance programs must secure resulting data streams, ensure data privacy, and mitigate the risk of digital surveillance.

Key Considerations for Cybersecurity Activities in DFS:

» Understand partner country policies, strategies, and regulations around cybersecurity, data privacy, communications infrastructure, and digitalization.

  ○ USAID Missions and Bureaus must understand the cybersecurity ecosystems they are operating in before designing and implementing new activities. Digital Ecosystem Country Assessments (DECAs) are one mechanism for better understanding these dynamics. If your Mission does not have a DECA, consider commissioning one.

» Include digital literacy and cyber hygiene training across all DFS programming. This will increase safety and build trust and confidence in the DFS products and systems. If specific partners need cyber hygiene training, consider buying into USAID's Digital APEX mechanism, which provides cybersecurity support to USAID partners. Use the email address below to contact the team for more details.

» Take steps to understand DFS provider practices. Do providers inform their customers about threats and cyber incidents? Do they introduce ways to easily identify or verify official communications, or include other product design features to help low literacy customers avoid threats? What is the quality of their customer care? How do they handle complaints and redress systems? Properly vetting DFS providers to ensure that they prioritize customer protection is critical, especially when DFS payments are supporting humanitarian assistance and other sensitive programs.

- Research should help to ascertain cybersecurity threats, vulnerabilities, and gaps at each level of the DFS ecosystem, for end-users, providers, and the systemic financial sector as a whole. Do DFS providers understand those risks?
- Build trusted initiatives that encourage local processes or frameworks for private sector DFS companies and other DFS stakeholders to share information on observed cybersecurity attacks or trends in the country or region.
- Coordinate with other donors to identify areas of alignment in cybersecurity for DFS.
- Embed cybersecurity considerations, resources, responsibilities, and management tools into every DFS project or activity.

FOR FURTHER INSIGHTS into the cybersecurity in USAID DFS programming, please reach out to USAID's Cybersecurity Team at cybersecurity.itr@usaid.gov.

Photo credit: Melinda Donnelly for USAID/Oceans