an online consumer chatbot, named BSP Online Buddy or BOB, where the public can submit their concerns and questions regarding their transactions with BSFIs," the BSP said.

"This is on top of the other available consumer assistance channels such as e-mail, snail mail, telephone/fax, and the Consumer Assistance Desk. Customer complaints received by the BSP's Consumer Affairs unit are referred to the concerned BSFI for appropriate action," it added.

Apart from raising consumer awareness, there has also been a campaign to continuously remind banks and other financial institutions of industry-wide best and up-to-date practices in improving cyber protection.

"Cybercriminal activities undermine public's trust and confidence in the financial system... During the pandemic, the BSP's approach in addressing cybersecurity challenges include providing a conducive environment for digital innovation, espousing vigorous cybersecurity measures, and promoting dynamic consumer protection mechanisms," the central bank said.

There have also been baseline assessments of the pandemic's impact to these financial institutions and their clients by constant surveillance of the operating and cyber threat environment, according to the BSP.

"From providing the necessary regulatory reliefs to fostering greater digital innovation, issuing coherent cybersecurity and technology policies, to ramping up cyber awareness campaigns for financial consumers, the BSP made sure that supervisory actions were risk-informed, data-driven and intelligence-led," it added.

The Bankers Association of the Philippines (BAP) also launched the BAP Cybersecurity Incident Database (BAPCID) as an information-sharing platform in 2019 which "proactively counter emerging cyber threats and raise overall situational awareness."

"Since the launching of BAPCID, participating BSFIs were able to have wider visibility on emerging cyber threats having access to threat intelligence reports and statistics. The BSP also uses the platform to share relevant cyber threat specific advisories and memoranda so BSFIs can proactively respond and do the necessary remediation to minimize potential impact and losses," BSP said.

The central bank further stretched its cybersecurity efforts with a new framework to be introduced this year.

"The BSP is currently developing a Cybersecurity Capability Maturity Model (CCMM) Framework consisting of four levels to facilitate cyber maturity assessment levels of BSFIs, with Level 4 as the most mature and Level 1 as the baseline. With this framework, BSFIs can chart their own progress and pinpoint specific areas where they need to improve to move to the higher level," the central bank said.

The regulator continues to closely monitor the capability of BSFIs to address evolving cyber threats and risks.

"For instance, cyber spending of BSFIs increased by as much as 43% from 2018 to 2019. This is a good indicator that BSFIs are putting greater emphasis on strengthening cybersecurity and in ascertaining the level of support and commitment of the BSFIs' board and senior management on cybersecurity concerns," said the BSP.

"Cybercriminals have taken advantage of the surge in the number of people using the bank's digital platforms. This mass migration to digital channels induced more criminals to shift to phishing and other related scams."

Maybank Philippines particularly enhanced its network and infrastructure cyber defense mechanism to strengthen its cybersecurity measures during the pandemic.

"As a leading financial institution within a global network, Maybank Philippines has long realized the impact of cybersecurity risks in its operations and have therefore made significant yet balanced investments in cybersecurity-related activities year on year," Ms. Del Rosario said, noting the bank took proactive activities to ease risks as well as appoint and scout the right people for their cybersecurity team.

For BPI, Mr. Paz said the bank has intensified its focus and investment on heightening public awareness, saying cybersecurity is a "shared responsibility."

"For fraudsters to be successful, they need user IDs, passwords, and the registered mobile numbers. The user IDs and passwords are usually captured via phishing e-mails and/or non-secure forms while mobile numbers are attacked either via taking control of the device (e.g., SIM swapping, device binding) and deceiving clients to divulge their OTPs or one-time-passwords," he said.

"The best defense against these attacks is public awareness," he added.

CONTENTS