# Why cybercrimes persist

https://opinion.inquirer.net/182026/why-cybercrimes-persist

Financial institutions supervised by the Bangko Sentral ng Pilipinas (BSP) lost P5.82 billion to cyberattacks in 2024, or 2.6 percent more than the P5.67 billion in 2023. The number of such crimes stood at 40,780 last year, slightly more than the 40,572 cases in 2023 but a worrying 151-percent jump from 16,246 instances in 2022.

The figures, presented by BSP Deputy Governor Chuchi G. Fonacier at the United Kingdom-Southeast Asia Tech conference last week, prompted Malacañang to express concern. “We are encouraging our banks to update their internal policies. On our part, we will conduct information dissemination about how people can avoid being scammed,” said Presidential Communications Office Undersecretary and Palace press officer Claire Castro. She stressed the need to update defenses against cybercrimes as technology continues to evolve, pointing out that “if crimes evolve, then we should also upgrade our measures against those crimes.”

The nagging problem, as always, is how. The country has Republic Act No. 11934, or the SIM Card Registration Act, signed into law by President Marcos on Oct. 10, 2022. It was meant to address the menace of text scams that proliferated particularly during the pandemic. Today, thousands of Filipinos still fall victim to different forms of text fraud and authorities seem helpless.

The Anti-Financial Account Scamming Act was enacted in July 2024 to address cybercrime, and the subsequent BSP Memorandum M-2024-029 was issued to plug the increase in fund transfers to unregistered third parties and unauthorized transactions and access to accounts, at the same time specifying employee and user accountability.

## Preventive, not curative

Still, cyber criminals continue to breed. It did not help that Congress, in crafting the 2025 national budget, had removed the P500-million allocation for the build-up of the Philippine National Police’s information technology system to boost the police’s capacity and skills to fight cybercrimes.

The point is that the government cannot do it alone. Stamping out cybercrimes is not solely the government’s responsibility. Banks and other financial technology companies should carry a big part of the burden in preventing cyber criminals from using vulnerabilities in their systems. Emphasis must be put on the need to act even before a scam is perpetrated. In other words, it must be preventive, not curative. Note that the second highest cybersecurity risk faced by BSP-supervised institutions last year was “card-not-present” (CNP), or remote purchase fraud wherein criminals use stolen or compromised credit card information to buy online or over the phone where the physical card is not needed. This accounted for P1.5 billion of the losses reported by banks last year.

## Red flags

Take the case of one recent victim who posted on social media how she was billed more than P240,000 worth of unauthorized purchases on her credit card even before she actually used it. It appeared that her card was cloned—or copied from the real one—and when activated using the bank’s official app, the criminals wasted no time in using up its credit limit. The red flags: How did the scammers get hold of the real credit card and clone it? Why was there no one-time PIN sent to the victim’s mobile phone number or verification check regarding the big purchases charged to the card?

Obviously, banks cannot pin this problem on their customers. Banks need to be stringent in their credit card operations as this case is one involving a breach in the issuing bank’s system. The BSP should bear hard on banks and penalize infractions with hefty fines.

An equal part of the burden must also be borne by consumers themselves. The highest cybersecurity risk reported by financial institutions last year was phishing, which accounted for P1.8 billion of the losses.

## Multilayered defenses

At the risk of being repetitive on how to avoid scams, the BSP advises everyone to be wary of emails or text messages asking for personal or financial information, especially if they seem urgent; be suspicious before clicking on any link; not to share account numbers, passwords, PINs, or other personal information, especially over email or text; transact only with legitimate online vendors, and be careful about the information shared on social networking sites.

The financial technology world is replete with ways on how to address cyber crimes. IT security experts specifically suggest strengthening cybersecurity systems, enhancing collaboration among players, and minimizing third-party risks by implementing multilayered defenses such firewalls, intrusion detection systems, endpoint protection, and the use of artificial intelligence-driven threat monitoring. The government must force financial institutions to implement these precautions now. As BSP’s Fonacier warned, “these incidents not only threaten to disrupt the delivery of financial products, but they also diminish the public’s trust in our budding digital financial ecosystem.”