- Computer crimes

At risk of cyberattack

Philippine Daily Inquirer · 7 May 2018 · A14

The rapid growth of the internet has led to many financial transactions being done online, such as banking, shopping and many other trading activities. As expected, devious individuals and groups find ways to steal money coursed through the internet. The Philippines has been among the countries identified as most vulnerable to this modern-day thievery commonly referred to as cyberattacks. Among the most common cybercrimes are identity theft, hacking (privacy intrusion or unauthorized use of private data), and distribution of malware to disrupt online services.

Last week, the Department of Information and Communications Technology (DICT) said that on a scale of A to E with "A" as the highest in terms of cybersecurity maturity, the Philippines was for now mostly in class "D," basically reacting to attacks with the available tools and technologies. In contrast, those in the "A" category are nationstates "resilient in times of cyberattacks." Last year, a study conducted by software giant Microsoft in the Asia-Pacific also found that the Philippines was the eighth highest in terms of encountering malware, which attacks computer operating systems to disable devices. Bangladesh, Cambodia, Indonesia, Myanmar and Vietnam were the top five most exposed countries in the region to malicious programs, according to Microsoft's Asia-Pacific office.

In the third quarter of 2015, the Philippines was likewise ranked 33rd out of 233 countries prone to cybersecurity threats, 10 spots worse from just the previous quarter. Internet security company Kaspersky noted in a report that the country experienced a rapid rise in malware infections for July, August and September in that year; it added that 17 percent of Filipino internet users were "infected" by malicious programs. On a global scale, it warned that mobile threats and attempted theft in online banking were also increasing. "From 43rd place to 33rd place in just three months shows that cyberattacks against the Philippines are accelerating at full speed. The Philippines may not be one of the top targets yet, but there is no doubt that cybercriminals are now noticing the country," a Kaspersky Lab Southeast Asia official pointed out.

True enough, in the following year, 2016, the Philippines figured prominently in the $81-million cyberheist involving funds stolen from the central bank of Bangladesh and laundered in the Philippines through the then unregulated casinos.

It is not that the Philippine government had been doing nothing to address this growing menace. Six years ago, Republic Act No. 10175, or the Cybercrime Prevention Act of 2012, was passed to address the cybercrime threat. A major factor for the initiation of the legislative measure was a report from Symantec, an internet security firm, showing that 87 percent of Filipinos had been victimized by cyberattacks. The law also seeks to help the gov-

ernment protect and safeguard the integrity of computers, communications systems, networks databases, and the confidentiality and safety of data stored in them from abuse, misuse and illegal access.

From a legal perspective, information technology experts agree that the Philippines could even be ahead of other countries because of the Data Privacy Act, the Electronic Commerce Act and the Anti-Wiretapping Law, aside from the Cybercrime Prevention Act. The problem is that many Filipinos are not familiar with the numerous threats in cyberspace.

The Bangko Sentral ng Pilipinas has been effectively advising and monitoring banks, which are considered targets of cybercriminals, to ensure they are well-protected against attacks. What should be addressed is the growing problem involving individuals and companies with very little knowledge or regard for cybersecurity. Hopefully, the DICT's launch this year of a national cybersecurity platform, which is to serve as the main base for cybersecurity initiatives, will help protect them. For the moment, it is advisable for everyone to be vigilant and aware of the many threats lurking on the internet.