# PRIMER ON CYBERCRIME

*This primer, outlined in a question and answer format, aims to make the Filipino public aware of the nature, history and extent of cybercrime occurrence in the country. It also makes the people informed of the latest development in anti-cybercrime efforts and activities by the Philippine Government.*

1) What is a cybercrime?

   A cybercrime is a crime committed with or through the use of information and communication technologies such as radio, television, cellular phone, computer and network, and other communication device or application.

2) How is a cybercrime different from a real-world crime?

   The main difference between a cybercrime and crime committed in the physical world is that cybercrime is committed with or through the use of information and communication technology. Furthermore, cybercrimes are punishable under special cybercrime laws and subject to distinct law enforcement provisions.

3) What are the types of cybercrime?

   There are various types and kinds of cybercrimes. The 2001 Budapest Convention on Cybercrime categorizes cybercrime offenses into four: (1) offences against the confidentiality, integrity and availability of computer data and systems; (2) computer-related offences; (3) content-related offences; and (4) offences related to infringements of copyright and related rights.

4) What is the global trend of cybercrime?

   Cybercrime is one of the fastest growing crimes globally. According to Norton Cyber Crime Report, 431 million adults worldwide were victims of cybercrimes in 2011. The costs that cybercrimes caused in 2011 amounted to $114 billion. Globally, the top cybercrimes in 2011 were (1) computer

viruses or malware - 54% overall; (2) online Scams - 11% overall; and (3) phishing - 10% overall.

5) What is the trend of cybercrime in the Philippines?

   In a 2010 report of the security software firm Symantec, 87% of Filipino internet users were identified as victims of crimes and malicious activities committed online. The following activities were: (1) malware (virus and Trojan) invasion; (2) online or phishing scams; (3) sexual predation; and (4) services in social networking site like Facebook and Twitter.

   The Anti-Transnational Crime Division (ATCD) of the Criminal Investigation and Detection Group (CIDG) of the Philippine National Police (PNP) has encountered 2,778 referred cases of computer crimes from government agencies and private individuals nationwide from 2003 to 2012.

6) What are the cybercrime-related laws in the Philippines?

   The cybercrime-related laws in the country are:
   (1) RA 10175 – Cybercrime Prevention Act of 2012, which is currently suspended due to a TRO issued by the Supreme Court; (2) RA 9995 - Anti-Photo and Voyeurism Act of 2009; (3) RA 9725 - Anti-Child Pornography Act of 2009; (4) RA 9208 - Anti-Trafficking in Persons Act of 2003; (5) RA 8792 - E-Commerce Act of 2000; (6) RA 8484 - Access Device Regulation Act of 1998; and (7) RA 4200 or Anti-Wiretapping Law.

7) What and when was the first recorded cybercrime in the Philippines?

   In 2000, Onel de Guzman released the “I Love You” virus. The case filed against De Guzman was dismissed at the first stage because there was no law punishing the deed as of that time in May 2000, in the Philippines.

8) When was a law penalizing computer crimes or cybercrimes passed?

   On 14 June 2000, RA 8792 or the Electronic Commerce Act was signed into law. RA 8792 positioned the Philippines as the third country to enact an e-commerce law, next to Singapore and Malaysia. The E-Commerce Act placed the Philippines on the list countries which penalize cybercrime.

9) In the Philippines, have we already convicted a cybercriminal?

   Yes. The first one was pursued by the PNP-CIDG; a person was convicted in September 2005 for pleading guilty of hacking the government portal "gov.ph" and other government websites. The NBI pursued a cybercrime case that led to the second cybercrime conviction; the person used the BPO call center provider Sitel Philippines Corporation to illegally secure credit card information from the company's sister firm, Sitel USA. The two convictions were secured under the Section 33(a) of RA 8972 that penalizes hacking.

10) What is the latest development in anti-cybercrime effort of the Philippine government?

   President Benigno Aquino signed into law RA 10175 or the Cybercrime Prevention Act of 2012 on September 12, 2012, which adopted the provisions of the first International Convention on Cybercrime. But the implementation of the new law which started on October 3, 2012 was put on hold after 6 days, when the Supreme Court issued a temporary restraining order against the law last October 9, 2012, after 15 petitions were filed against it.

   As of the moment, cybercrime-related cases are dealt with using existing laws.