# Crime Hidden in Email Spam

4

**Szde Yu**
*Wichita State University, USA*

## INTRODUCTION

Crime on the web has gained significant attention in recent years. In the past, the study of cybercrime was not exactly new but it was by no means a focal concern in the mainstream criminology. Nowadays, however, it seems every crime could have a cyber-related component in it and therefore potentially all crimes can be committed or facilitated by the use of cyberspace. For example, even though you still cannot murder or rape someone on the Internet, you could stalk your victim on the Internet beforehand or you could video-record the crime and sell the footage in the black market. Typically such online black markets exist on the so-called Dark Web or Deep Web. On the Dark Web, you can advertise anything you have to offer or you might find anything you need with a price. Conceivably many things happening on the Dark Web are not legal. Otherwise, they could have simply done the transaction on Amazon.com. In other chapters, the definition of the Dark Web has been provided and how it functions has been discussed. Instead of repeating them, this chapter focuses on how information is being disseminated in the cyber-criminal-world since criminal activities on the Dark Web cannot be Googled. More precisely, the focus is on email spam and the role it plays in facilitating criminal activities that may or may not necessarily take place on the Dark Web. Email spam has long been dismissed as a trivial crime that does not usually warrant much attention from either academics or practitioners. Nonetheless, its low-profile status among crimes may have actually endowed email spam with the best utility in criminal communication.

## BACKGROUND

Email spam is defined as unsolicited commercial electronic mail that includes any commercial emails addressed to a recipient with whom the sender has no existing business or personal relationship and not sent with the consent of the recipient, and commercial electronic mail is defined as any electronic mail message the primary purpose of which is commercial advertisement or promotion of products or service (Rogers, 2006). Sending spam emails can be treated as a criminal offense in the United States, according to the CAN-SPAM Act enacted in 2003. The Act imposes penalties on sending unsolicited commercial email if the provisions set by the Act are violated. The Federal Trade Commission (FTC) is in charge of enforcement of these provisions and it also provides regulations of which any violation can be declared criminal (FTC, 2009). The FTC regulations are as follows: 1. Don't use false or misleading header information; 2. Don't use deceptive subject lines; 3. Identify the message as an ad; 4. Tell recipients how to opt out and honor opt-out promptly; 5. Monitor what others are doing on your behalf (FTC, 2009). In 2008, the so-called "Spam King" Robert Soloway was convicted under the CAN-SPAM Act and was sentenced to 47 months in federal prison (Rabinovitch, 2007). The Act also allows states and Internet service providers to file civil lawsuits against spammers (Ford, 2005; Yeargain et al., 2004). Despite this, email spam has never been seen as a serious crime even though email spam is probably one of the most

DOI: 10.4018/978-1-5225-9715-5.ch057

prevalent crimes as almost every person who uses email has received at least some unsolicited junk emails that aim at advertising, phishing or scamming. Most people tend to simply delete them or rely on the spam filter embedded by the service provider to screen them out. However, spam filters are not entirely reliable. As a result, users often have to check the spam folder to see if some important messages have been mistakenly flagged as spam (i.e., false positive). A false positive could cost a delay or omission in an important communication and sometimes this could entail significant consequences (Weinstein, 2003). Therefore, it is an understatement to say email spam is nothing more than a nuisance. In fact, email spam can be costly. Some research has indicated that the time and productivity wasted on account of email spam can amount to 20 billion dollars every year (Yeargain, et al., 2004). The energy used to transmit, process, and filter spam can be equivalent to the electricity used in 2.4 million households annually (McAfee, 2009). In addition, the cost of email spam can be much higher when it is being utilized as a communicative avenue for criminal purposes, such as scam, illicit drug selling, and sex crimes (Yu, 2015a). Unfortunately, the link between email spam and other crimes has long been overlooked. Accordingly, in this chapter the criminal activities associated with email spam are discussed regarding how email spam is being used by criminals to reach potential customers and victims.

## FOCUS OF THE ARTICLE

### Scam/Fraud

Money is a common motive behind a variety of crimes and email spam is one of these crimes. While many spammers send advertisements to promote commercial products, some spammers resort to scam or fraud. Some scam schemes are elaborate while others could seemingly lack sophistication. Many people are familiar with that Nigerian prince who is looking for someone to help him move money around, and he allegedly is so grateful that he is willing to pay the helper a whopping proportion of his fortune. In addition, many people are lucky enough to have won a lottery they do not remember buying, but no matter how big the winning prize is the lucky winner somehow is always asked to pay a processing fee first. Lately, scammers seem to prefer impersonation. They might pretend to be the IT department in your organization and ask for your passwords, or they could pretend to be your bank and ask for your account information. These schemes are getting old but at least the scammer is willing to make up a story. Some schemes are simply carried out in an email that has only one or two sentences, such as "you have a message; click here." However, they could work as well thanks to people's curiosity. Phishing is a very popular way of luring people to visit a website where the actual scam will take place so that the scammer does not need to disclose too much in the email. This method also allows scammers to remain hard to trace by using a false sender address or changing servers, because they do not need to wait for your reply. If they need to wait for the recipient to reply like the Nigerian prince usually would, it means the scammers have to stay active on the same email server for a while, which increases the odds of being caught.

Regardless of the scheme being used, in essence scammers are trying to acquire sensitive personal information so that they can either use it directly or sell it for profit. Figure 1 is an example of scam email. It is typical for scammers to try to establish contact by implying you are the chosen one but they cannot really address you by your name because this identical email was sent to possibly hundreds or even thousands of people at the same time, which is characteristic of email spam. This is especially true in the past when spammers mostly rely on a web crawler to collect email addresses randomly from