Fraud schemes. spam emails

Technology, Information Technology

Week 7 Individual Project Unwanted communication is nothing new. The telephone has been used to some extent but has almost died out over the past few years, due to the decline of land lines, seeing as how most cell phones are unpublished. Businesses and those people with fax machines also receive unwanted messages. But written correspondence has always been the most popular, starting with the posting of bills, a practice still ongoing in supermarket parking lots. Ever since the mail has been delivered, companies and " shady" individuals have sent unsolicited marketing materials to private address. From an inundation of Christmas catalogs to chain letters junk mail is still prevalent. As a matter of pact the US Postal Service is actually actively recruiting standard mail customers, due to decreasing first class profits (Nixon 2012). Yet as phones and mail have improved with technology, so has junk mail. There are even new terms to describe junk email, such as SPAM and phishing. Some can be mundane and even ridiculous, such as letters from " Nigeria" promising millions of dollars if one helps them to smuggle these funds from the country. Yet this is definitely illegal and even has its own name, the " 419 Fraud" for normally the scammer wants your bank account information so he can rip you off. As ludicrous as it sounds, thousands of people have fallen victim to this scheme (FBI 2012). If one knows what to look for there are several characteristics that most SPAM has in common (Red Earth 2012). First is quite obvious. As the vast majority of SPAM is in English the non native speakers can literally butcher the language. For example, 890929496. 24872 has many words running together and " Definetly not junk mail". The from and reply to addresses are not the same. Linus@vsource. com seems to send many

letters in this group. Yet the mail named 891219144. 5405 traces back to bguenter@gemprint. com, which also answers question number 2. This was not a firm at all but evidently a private person attempting to conceal his identity. By the way, Gemprint is a legitimate website specializing in jewel fingerprinting. Another characteristic is that the recipient’s address is not readily seen. This is seen also in 890929496. 24872, where it seems like fifty recipients are included. SPAM filtering devices on email servers are getting ever more sophisticated in their attempt to stay one step ahead of the spammers. So that leads to another characteristic that is prevalent in many SPAM emails. Not only do they use a lot of HTML, they use many comment tags which looks like in coding. The filters look for key spamming words and by using the comment tags, the spammers circumvent the filters. One more trick is the “ opt out” feature where you can decline to receive any more letters from this entity is just another way to get you to their website. In example, 891020028. 3223 uses double speak to let you opt out AND visit their site! Questions three is answered by Perimetec (2012), a leading provider of anti SPAM software for businesses. Eighty per cent of SPAM comes from just 200 people. Likewise, although when people think of spammers, they envision some hacker in a third world country. Actually the truth is twenty per cent of all SPAM comes from the United States, far usurping its closest competitor, China. Wonder if that means the English mistakes are deliberate? On the same token when shown by continents, Asia accounts for almost half of the SPAM generated (40%). Also in answer to question five, a lot of spammers prefer to use free commercial accounts such as Hotmail, Gmail and Yahoo. The reason is simple, one can have unlimited

email accounts using many fictitious names, whereas the pay servers require more stringent identity procedures. Phishing is definitely a problem. Using look alike emails from legitimate concerns like Chase, American Express and others, the phisher attempts to extract personal information from the mail recipient. Although SPAM is annoying, it is relatively harmless unless one visits the website and purchases something, phishing is yet another case of identity theft. So the FBI classifies it as interstate fraud (Ibid). Yet as with all SPAM, phishing can be identified by looking at the headers. For instance, one of my own SPAM e-mails today informed me I had won some obscure lottery worth $800 million! Using MS Outlook, by right clicking on the message (without having to open it), you can plainly see where the message originated from. Forensics investigators can then establish the originating IP address for the offending email. If in a friendly country the criminal can eventually be prosecuted as was the case with Jeremy Jaynes, sentenced in Virginia to nine years for sending some ten million SPAM emails (Hoffmann 2008). References: FBI, 2012, Common Fraud Schemes, viewed October 19, 2012, Hoffmann, Stefanie, 2008, CRN, Virginia Supreme Court Upholds First U. S. Spam Conviction, viewed October 19, 2012, < http://www. crn. com/news/security/206901452/virginia-supreme-court-upholds-first-u-s-spam-conviction. htm> Nixon, Ron, 2012, New York Times, Seeking Revenue, Postal Service Plans to Deliver More Junk Mail, viewed October 19, 2012, Perimetec, 2012, Where Does Most of the Worlds Spam Come From?, viewed October 19, 2012, < http://www. perimetec. com/all-about-spam/where-does-most-of-the-worlds-spam-come-from. php Red Earth Software, 2012, Top 10 SPAM Characteristics, viewed October 19, 2012,