

Sidney Bloxom Scholarships

Trends of Economic Crime

By: Lance Erickson

#85 P.O Box 6500

Regina, Sask

S4P 3J7

(306) 949-6549

Grade 10
Regina Christian School

Trends of Modern Economic Crime

Economic crime has evolved exponentially in the last two decades with the rapid development of computers and the Internet. Scams that would have taken weeks to months to accomplish can now be dealt out in seconds with little or no effort and cost to the scammer. Three of the more popular trends in economic crime these days are: Spyware/Malware, Identity Theft, and 'Phishing'. All three of these scams utilize two major tools: Social Engineering (the art of getting information from the source) and Technological Exploits (software exploits). Utilizing modern technology and old fashion know how, spyware, identity theft, and phishing have become the most prevalent economic crimes.

Spyware and its more malicious cousin, malware, are the most prevalent and controversial scams in existence. Often found piggy backing on larger software programs (ie: KaZaa), spyware and malware install themselves on a victim's computer without the user's knowledge or consent and collect information to send back to its mother company. This information can then be used for a variety of purposes, depending on the company, like selling it out for profit or for advertising purposes. The problem is not all spyware is malicious to the point of collecting personal information, but some are, making it increasingly hard to identify the potential risk. This controversy has led 'spyware' companies to sue users who call their software spyware, claiming it isn't. Specifically, spyware that collects and sends personal information for malicious purposes is called malware. Malware can be used to collect information that can lead to identity theft.

Identity theft has been around for decades, what has changed though is the way the scammer gets his/her hands on the victim's personal information. Utilizing the Internet and some social engineering skills, a scammer can collect enough information to convince vendors & banks that he/she is the victim in a matter of days, all from the comfort of their own home. Once a victim's identity has been stolen, it can be extremely

hard to reverse the damage that has been done and get back the money and bank credit that would have been lost. Though not as serious as identity theft, 'phishing' has become one of the most prevalent and dangerous economic crimes.

Phishing, of the three scams, can be the most dangerous because of how easily it can be deployed and how convincing it can be. A phishing scam (comparable to the Nigerian dictator scam) involves sending a potential victim an official looking e-mail message asking for some sort of information claiming to be a legitimate company. These can take the forms of fake *Paypal* messages asking for account information. This e-mail could then lead the victim to a very official looking site where, utilizing a security exploit in certain Internet browsers, the URL is masked so that it reads official site's URL, instead of its actual URL. The victim, thinking that they are sending info to a legit site, would actually be sending it to a scammer who would then use this to take over the victim's account and remove the funds from it. The whole scam can take less than a day to deploy yet could cost the victim thousands.

From the controversial spyware problem, potent identity theft, and costly phishing scams, economic crime has evolved dramatically from its roots. Technology has made identity theft and phishing faster and easier to deploy and has allowed spyware and malware to cleverly operate under the public radar. These three scams are prime examples of the state of modern economic crime.