Unethical decisions

Technology, Information Technology

Unethical decisions With respect to the growing technological advancement, there has been complimentary rise intheft and fraudulent activities spurred majorly by the same good technology. The rise in fraudulent activities has since centered the world in big problems ranging from job loss to loss of large amount of funds. The following paper illustrates particular technological innovations that have faced setbacks occasioned by increased internet and technological fraudulence. The paper will then conduct explicit research on the possible ways of detecting and avoiding cases of fraudulence

The growing technological advancement has led to integration of the communication all over the world. Integrated information system has been a great relief to many people as well as organization when it comes to conducting electronic transactions. However, this development has been met and strained by serious unethical practices that have led to great loss of finances and jobs. Unethical practices and decisions made on the information systems have also led to disrepute to many organizations (Collier & Spaul, 1990).

The integration of information system witnessed an advantageous introduction of credit cards that have been used to carry transactions involving purchasing and sales of goods and services. However, this system has since undergone intrusion occasioned by unending frauds (Shortland & Scarf, 2007). Credit cards of certain individuals have been stolen and used in purchase of goods and services by the fraudsters, thus leading loss of colossal amounts of money by the credit card companies. The same problem has been witnessed even with the use of virtual credit cards. Fraudsters have

used complex techniques to get to know the secrete information of the credit cards of particular individuals and have been conducting transactions with such cards at the expense of the true holders.

To confront, tackle and curb credit card frauds, Shortland and Scarf (2007) illustrate that various individuals have come with systems to assist achieve the alleviation of these widespread unethical practices. The ideas have included metalearning, and cardwatch among others that uses modifiers and classifiers to mine data and detect frauds in the system. Even though, these technologies have failed to bear desirable fruits as disorganized distribution of data and mixing of the genuine and fraudulent transactions that have complicated the functionality of the systems. Continuing research on this field has led to invention of the Hidden Markov Model (HMM) that works effectively by detecting frauds through consideration of the spending habits of the card holder (Shortland & Scarf, 2007). The system collaborates with the banks that the card holder uses to pay for goods and services. When any irregularity is detected in the spending pattern then the HMM system alerts the banks that serves the particular client (Shortland & Scarf, 2007).

According to Ajah and Inyiama (2011), the field of information system has also faced emergence of fake websites made to resemble an exact websites of big financial institutions that carry large transactions of money. Fake websites exists in various forms common of which are the spoof and concocted sites. Spoof sites have been made to resemble the eBay, PayPal and many other international banks. The appearance of the spoof sites is designed to hoodwink clients dealing with particular financial institutions and drive them into conducting transaction with such sites. Such acts lead to

automatic loss of money. The concocted sites on the other hand are made to resemble the real shipping company, online retailers and investment banks. The fraudsters operating such sites invite customer to order and pay for goods, which not be delivered to the customers.

To avert and avoid the effects of the fake websites, technologists have come up with integrated software systems installed in the client server computers with blacklists of all fake websites. Whenever such websites want to appear on the client server computers, they get blocked and averted from corrupting the system. The popular software that has since been developed to accomplish the tasks includes the Sitehound and Cloudmark among others (Ajah & Inyiama, 2011). There are also special classifiers that determine the fraud cues present on a particular website and with reference to the available blacklist, blocks any website perceived as threat. Coderre (1999) indicates that there are also certain special computer programs like the CAAT that helps financial auditors detect any element of inappropriate transactions. The CAAT program scrutinizes the salaries paid to particular employees within a certain time frame together with the taxes charged on every transaction to detect any symptoms of misquotation of figures. Computer assisted fraud detection also involves the use of FCI that assists in detection of frauds present in contracts and purchases (Coderre, 1999).

In conclusion, information systems have from time to time attacked and corrupted by certain fraudsters with the intention of steeling and hacking essential data from the victim’s websites. However, the trend of fraud has been decreasing substantially as new technological ideas have been developed to help curb the risks. Even though some mechanisms have not

been productive, some have served very to ensure maximum achievement of the missions of eradicating frauds in the information systems.

References

Shortland, R., & Scarf, R. (2007). Data mining applications in BT. BT Technology Journal, 25(3-4), 272-277

Ajah, I., & Inyiama, C. (2011). Loan Fraud Detection And IT-Based Combat Strategies. Journal Of Internet Banking & Commerce, 16(2), 1-13.

Coderre, D. (1999). Computer-assisted techniques for fraud detection. The CPA Journal, 69(8), 57-59.

Crowder, N. (1997). Fraud detection techniques. The Internal Auditor, 54(2), 17-20.

Collier, P. A., & Spaul, B. J. (1990). Information systems forensics. Journal of Information Technology, 5(3), 134-140.