Phinney, J. S., Horenczyk, G., Liebkind, K., & Vedder, P. (2001). Ethnic identity, immigration, and well-being: An interaction perspective. *Journal of Social Issues, 57*, 493-510.

Solomon, S., Greenberg, J., & Pyszczynski, T. (2000). Pride and prejudice:Fear of death and social behavior. *Current Directions in Psychological Science, 9*, 200-204.

Swartz-Kulstad, J., & Martin, W. (1999). Impact of culture and context on psychosocial adaptation: The cultural and contextual guide process. *Journal of Counseling and Development, 77*, 281-293.

Tajfel, H. (1981). *Human groups and social cate gories*. Cambridge, England: CUP.

Tajfel, H. (1982). Social psychology of intergroup relations. *Annual Review of Psychology, 33*, 1-39.

Tajfel, H., & Turner, J. (1979). An integrative theory of intergroup conflict. In W. Austin & S. Worchel (Eds.), T*he social psychology of intergroup relations* (pp. 7–24). Monterey, CA: Brooks/Cole.

Tajfel, H., & Turner, J. C. (1986). The social identity theory of intergroup behaviour. In S. Worchel & W. G. Austin (Eds.), *Psychology of inter group relations* (pp. 7–24). Chicago, IL: Nelson-Hall.

Yakushko, O. (2009). Xenophobia: Understanding the roots and consequences of negative attitudes toward immigrants. *The Counseling Psychologist, 37*(1), 36-66.

Yeh, C.J., Kim, A.B., Pituc, S.T., & Atkins, M., (2008). Poverty, loss, and resilience: The story of Chinese immigrant youth. *Journal of Counseling Psychology, 55*(1), 34-48.

About the Author:
Michael Sapiro has a Master's in English with a focus on social justice and feminist pedagogy and is currently working toward his PsyD in Clinical Psychology from JFK University in California. He is on the Board of Directors for the Institute for Spirituality and Psychology and teaches workshops on the intersection of psychology, spirituality and social justice.

* * *

Internet Fraud: Information for Teachers and Students

Gabriel Hudson Nkotagu
Arkansas State University – Jonesboro
gabriel.nkotagu@smail.astate.edu

Abstract

Internet fraud takes a number of forms with the responsible individuals changing tactics rapidly to avoid detection. The perpetrators rely on telemarketing, emails, as well as presenting themselves personally to unsuspecting people. The evolution of internet marketing as well as ecommerce and the ease of connectivity create increasing opportunities for fraudsters while at the same time placing more unsuspecting internet users at risk of falling prey to these schemes. There exists a thriving economy online with large sums of money changing hands online. It is therefore important for any internet user to easily identify when they are exposed to internet fraud schemes and as such avoid being a victim.

Internet Uses

The internet is important as it provides an avenue as well as a backbone for electronic commerce, research, communication, and education. It provides information ranging from full books to journals, all of which are important to teachers and students. Research for instance can be very difficult if the information present in online databases was not available. Apart from educational use, students as well as teachers participate in communication through social networks, electronic mail, as well as voice communication such as Skype.

Risks of Using Internet

Use of the internet may expose both teachers and students to many risks ranging from identity theft, fraud, and exposure to malware that can easily result

in harm to the users. The presence of unlimited connectivity often results in students spending considerable amounts of time online thus increasing the risks of being prey to fraudsters (Nikitkov & Bay, 2008). The possibility of falling victim to fraud is always high especially if one is unaware of the existence of internet fraud. Many international students and teachers are more susceptible to online fraud, as some have had little access to unlimited connectivity prior to joining schools overseas. Some international students and teachers may not know that the internet can be used to deceive and swindle them out of their money or even steal personal information. Many users use the service without taking any precautions, especially on unsecured auction websites (Mohatar & Sierra Cámara, 2007).

Unrestricted web use often leads students to websites that participate in fraudulent activities thus exposing them to a risk of being scammed. A search for a particular textbook for instance could lead a student to an online auction website where the book is offered. Pressure from teachers and need for the book can simply lead an individual to buy it from the website exposing him/her to the possibility of being a victim of fraud if (Hache & Ryder, 2011).

Forms of Internet Fraud

Internet fraud takes a number of forms with perpetrators currently relying on telemarketing, emails, and presenting themselves personally to unsuspecting people met in online chat rooms or social networks. The evolution of internet marketing as well as e-commerce has increased opportunities for fraudsters. There exists a thriving economy online for these scammers, making it a necessity for international students and teachers to have skills for early detection of fraud. Unfortunately, this detection happens when it is too late. This is due to lack of proper training on safe use of the internet (Brown, 2011).

The most common form of online fraud occurs through sale or advertisements of goods and services that do not exist. International students are more likely to fall prey as they have a desperate need for many products not sold locally. They end up giving away their credit card information to buy those products. Most of the time however, goods and services paid for are not delivered to the buyer. This common occurrence has seen many students and teachers lose money to fraudsters. Early detection is possible and can result in the reimbursement of funds if reported immediately to the bank issuing the credit or debit card.

Other online sellers create false statements about their goods and services with products delivered. Generally, fraudsters make online auctions look legitimate and tailor them to attract foreign students who are yet to learn how online fraud happens. All information provided by the seller is assumed true in online trade, as a buyer cannot physically see or inspect the goods. Online traders all over the world are however flouting this rule (Roddel, 2008).

Other online auction sites include hidden fees. This results into buyers paying more than what they expected (Hu, Liu & Sambamurthy, 2011).

Another form of fraud comes in the form of phishing. This occurs when spam mails are sent to unsuspecting individuals. Scammers usually pretend to come from a company or organization that is well known. Phishing is soliciting personal information that can be used to steal an individual's identity as well as information related to banking that can result in loss of funds through credit card purchases that are unauthorized. One example of such an email is the recent phishing done with the aim of getting individuals to divulge their PayPal account details (Chua, Jonathan, & Daniel, 2007). Addresses from which the emails were sent were created from the Google email service, Gmail, which pointed directly to phishing. Many individuals replied to the mail and this led to the eventual loss of funds from their accounts.

Vishing is another concept where phone calls are made with the caller pretending to be from a financial or banking institution that the victim uses. In this way, an individual unknowingly divulges banking details (Brown, 2011). Another form of online fraud is identity theft. Theft of an individual's identity is done with the aim of stealing money from them (Frank & Paul, 2011). Possible use of identities can be bank fraud where an individual's personal information is presented in a bank and used to acquire large loans. The loans go unpaid prompting the bank to make follow-ups in this case following the real owner of the identity who is largely unaware of the occurrence (Natalita, Maria & Marian, 2011).

Others include subscriptions which appear to be one-off purchases but which later on result in individuals unknowingly paying money every month or every scheduled period of time (Christou et al. 2011). The companies involved in this simply continue deducting funds from an individual's credit card, an event that can go unnoticed for a very long time. International students are at a risk of falling prey to this simply because these subscription services are tailored to appear as cheap one-off purchases.

Precautionary Measures

In spite of all the loopholes presented by the internet, it is possible to avoid being a victim of fraud. Taking precautionary measures is a step toward ensuring safety on the internet (Hintze, 2011). Introduction of safe use of the internet, especially for international students, remains important to ensure safety from online fraud.

The following are things to look for before accessing any website (especially ones that ask for credit card information). Students can verify safety of websites by ensuring that all websites used for online payments or banking are registered under companies with physical addresses that are accurate and present at the time of payment (Chang & Chang, 2011). The time the company has been in operation as well as the time the website has been online is also an important aspect to note. This information is available from several sources on the internet. Secure websites normally have a small padlock symbol as well as the wording https just before the URL to the site (Gavish & Christopher, 2008). Also these websites should have some form of policy, which should always be read prior to making any transaction. Online trading websites should also have return policies for products.

It is a common rule that information solicited over the phone or through websites is not given if one is unsure of the individual asking for it. Sensitive information should not be given out just because a service requests for it. The lure of buying products at a cheap price as well as the promise to make money or simplify processes as in the case of vishing is responsible for many losses. Lack of knowledge on the issue of internet fraud makes international students easy prey for these schemes. Payments made online can be secured by use of escrow services to ensure that products are delivered to the buyer before releasing any money to the seller (Thomas, 2010).

Conclusions

International students and teachers need to ensure that they conduct research prior to investing online or carrying out any other transactions (Dinew, 2006). Every day new methods to defraud people are being devised and this simply places people at a risk of falling prey to online fraud schemes. Knowing when one is a victim is an important step if the culprits are to be caught. Logging in to online accounts regularly, subscribing to notifications of account activity, as well as regularly changing passwords is important to ensure fraudsters do not access information one owns. If one discovers that bank statements show deductions they are not aware of, then they might be possible victims of bank fraud. International students are likely to fall prey especially to auctions as they are used to making purchases from shops so the thrill of buying items online can be overwhelming. Enlightening them of the possible loss of money online is an important step to bringing them closer to avoiding fraud (Frank & Paul, 2011).

References

Brown, E. (2011). Internet law in the courts. *Journal of Internet Law, 12*(7), 22-25.

Chang, W., & Chang, J. (2011). A novel two-stage phased modeling framework for early fraud detection in online auctions. *Expert Systems with Applications, 38*(9), 11244-11260.

Christou, I. T., Bakopoulos, M. M., Dimitriou, T. T., Amolochitis, E. E., Tsekeridou, S. S., & Dimitriadis, C. C. (2011). Detecting fraud in online games of chance and lotteries. *Expert Systems with Applications, 38*(10), 13158-13169.

Chua, C. E. H., Jonathan, W., & Daniel, R. (2007). The role of online trading communities in managing internet auction fraud. *MIS Quarterly, 31*(4), 759-781.

Dinew, T. (2006). Why spoofing is serious internet fraud. *Communications of the ACM, 49*(10), 77-82.

Frank, S., & Paul, W. (2011). Understanding scam vic tims: Seven principles for systems security. *Communications of the ACM, 54*(3), 70-75.

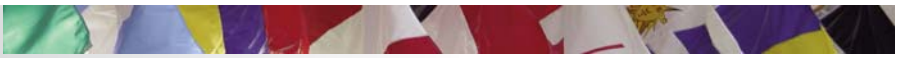
Gavish, B., & Christopher, L. T. (2008). Reducing internet auction fraud. *Communications of the ACM, 51*(5), 89-97.

Hache, A., & Ryder, N. (2011). 'Tis the season to (be jolly?) wise-up to online fraudsters. Criminals on the web lurking to scam shoppers this Christmas: A critical analysis of the United Kingdom's legislative provisions and policies to tackle online fraud. *Information & Communications Technology Law, 20*(1), 35-56.

Hintze, J. (2011). Beware online banking thieves. Retrieved from *www.treasuryandrisk.com*

Hu, N., Liu, L., & Sambamurthy, V. (2011). Fraud detection in online consumer reviews. *Decision Support Systems, 50*(3), 614-626.

Mintz, P. A., & Steve, F. (2002). *Web of deception: Misinformation on the Internet.* New York: Information today.



Mohatar, O., & Sierra Cámara, J. M. (2007). New directions in online fraud. *AIP Conference Proceedings, 963*(2), 973-976.

Natalita, M. S., Maria, E., & Marian, E. (2011). Challenges of managing e-commerce. *Economics Management and Financial Markets, 6*(2), 194-199.

Nikitkov, A., & Bay, D. (2008). Online auction fraud: Ethical perspective. *Journal of Business Ethics, 79*(3), 235-244.

Roddel, V. (2008). *The Ultimate Guide to Internet Safety*. New York: Lulu.

Thomas, B. (2010). Simple precautions reduce risk of online financial fraud. *Retrieved from http://www.hackerjournals.com*

About the author:
Gabriel Hudson Nkotagu is an undergraduate student from the United Republic of Tanzania at Arkansas State University.

***