6

THE MANY FACES OF CYBER-CRIME: THE IMPLICATIONS ON E-BANKING

Ayo, C. K. (Ph.D),*
and
Babajide, Daniel Olutope**

*Dr. Charles Korede Ayo holds a B.Sc, M.Sc and Ph.D. in Computer Science. He is currently the Head of Department of Computer and Information Science, College of Science and Technology, Covenant University, Ota. He is a member of the Nigerian Computer Society (NSC) and Computer Professional Registration Council of Nigeria (MPC). E-mail: ckayome@yahoo.com

**Mr. Olutope Daniel Babajide (BSc) is currently a Graduate/Research Assistant, Computer and Information Sciences, Computer and Information Science Department, College of Science and Technology, Covenant University, Ota. E-mail: tunjibabajide@yahoo.com.

ABSTRACT

Technology, particularly IT has brought to mankind a number of features and service delivery channels aimed at offering convenience, enhanced productivity and profitability but not without trade-offs. Crime, fraud and insecurity are some of the associated snags which have hindered in no small measure the wide application of IT.

This paper reviews the different forms of crime perpetrated through IT, the effects on e-banking and the possible solutions for a wider acceptability.

KEYWORDS: **CYBER-CRIME, CYBER-TERRORISM, CYBER-EXTORTION, PUBLIC KEY INFRASTRUCTURE, AND PREVENTIVE MEASURES.**

1.0 INTRODUCTION

Before the popularity of computer networks and the Internet, the vulnerability of PCs to virus and worms was reduced to exchange of diskettes among users. However, with the advent of the Internet and its increased use in business transactions, the vulnerability of these connected systems has been on the increase.

Beside viruses and worms, there are a number of activities that constitute severe threats to e-banking. Fraud manifests in a number of ways such as identity theft, phishing, worms, hacking, cracking,

hijacking, spywaring, card forgery, repeated cash withdrawals, slip fraud, ATM fraud, skimming, multiple payment of services and goods as well as stolen or lost cards fraud (Vladimir, 2003).

One of the biggest problems of insecurity is caused by the broadband internet access where systems are left online 24/7. Thus cyber-criminals cash in on this fact to exploit gaps in security networks to defraud both individuals and corporate organizations, while virus and worm attacks were prevalent in a dial-up connection, this problem is compounded in broadband access because of the possibility of a third party to have access to the system (Smith, 2004).

Generally, to match the increase awareness and acceptability of the net, there is a relative boost in cyber-fraud. Hence it has become the preferred tool for criminals and terrorists to attack the unsuspecting user.

The Internet has provided a virtual battlefield for countries to settle their scores. Particularly Taiwan against China, Israel against Palestine, India against Pakistan, China against US and Iraq against US among others (Elmusharaf, 2004).

2.0 E-FRAUD

This is a kind of fraud that is perpetrated through the electronic gadgets. It includes: cyber-crimes, viruses and worms, and cyber-terrorism.

2.1 CYBER-CRIME

These refer to all forms of crime perpetrated through the internet. It is otherwise referred to as Internet fraud. That is, using one or more component of the Internet such as Chat rooms, E-mail, Usenet and the Web, among others, to present fraudulent solicitations to prospective victims in other to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions (Babu, 2004). This fraud is carried out under different names as listed below (Guerin, 2004):

Merchant Fraud

This occurs through a dishonest staff or fake merchants that collude with fraudsters to defraud unsuspecting clients. It is either that the staff transmits the client's credit card information to fraudsters who take over his account immediately or the merchant himself puts up a fake site with the intension of collecting the clients' card information.

Cardholder fraud

Fraud perpetrated by cardholder through their payment cards. Clients, after receiving the goods purchased instruct their banks to stop payment on the ground that they did not receive the goods or that the transaction is under dispute.

ATM fraud

This fraud is now very reduced because of the mandatory use of four digit PINs verifiable online. The fraud is perpetrated by capturing the contents of the magnetic stripe as the card is inserted into the reader, and where such means is not available the fraudsters resort to "shoulder surfing" looking out for the cardholder's PIN. Other forms of ATM fraud are:

- **Skimming**

  This involves copying the cardholders' PINs to create a counterfeit copy and distribute abroad for fraudulent intentions. This is called "white plastic"

fraud. The fraudsters reproduce the magnetic stripe on a blank card and work in collusion with a merchant.

- **Credit Card theft**

Cards are stolen and used quickly to make several purchases until the loss is reported and blocked. Such cards can be distributed abroad particularly in countries where there is poor telecommunications network.

- **Counterfeit Card Fraud**

This entails generating PINs randomly and produces cards using embossing equipment. It is a very organized crime.

- **Card-Not-Present Fraud**

The card-not-present environment is very risky. There is no physical contact among the parties and telephone or the web is the only means of interaction, and either of them can fake his identity.

- **Mail Order Telephone Order (MOTO) fraud**

MOTO presents a cheaper way of transacting business by mail devoid of physical outlet. This environment is risky because the billing address may not match the delivery address. An up-to-date telephone register helps to reconcile addresses to certain extent.

- **Internet fraud**

Criminals capitalize on the anonymity and the global reach of the Internet to perpetrate fraud. It is difficult enacting laws binding on fraudster because it is international in nature.

- **Identity Theft**

This is greatest threat to e-banking and e-commerce. It represented about 43% of all complaints made to the federal trade commission (FTC). This involves insiders selling private information to fraudsters or through junk mails to fake an unsuspecting client.

However, phishing, worms, hacking, highjacking and spyware are the quintet of criminal activities currently plaquing the consumer side of the Internet (Gould, 2004).

Phishing is a relatively new kind of scam, which means swindling out confidential data from trusted and unsuspecting users (Dmitri, 2004). Criminals can create a counterfeit website and send a false-alert to all consumers and call for a re-registration with the intention of stealing their identities.

Pharming is a system that misdirects web users of trusted brands to phony storefronts setup to harvest IDs.

Worms are like computer viruses but have the capability to copy both corporate and user passwords from the victim (financial institution). Some may usurp the resources of the computer and eventually pack it up.

Hacking attacks are even more frequent and successful. This involves direct attack on PCs to extract identity and financial account data.

Spyware is a system that tracks the actions of a user and/or their Internet use. It captures all information entered through the keyboard including passwords and transmits same to the fraudsters.

Adware is similar to spyware that collects information about the user in order to display advertisements in the web browser based on the information.

Scumware changes the way websites are displayed. It replaces the actual contents of the site with adverts of the scumware, and generates traffic for such adverts.

Spamware is a software that mails unsolicited mails (junk mails) to people online. This may end up being any of the fraudulent mails (virus, worms etc).

2.2 VIRUSES TROJAN HORSES AND WORMS

All these have become a major threat to e-banking and e-commerce. They waste disk space, delay computer operations with increased possibility of system crash.

A computer virus is a manmade virus which is a software that has the capability of replicating by attaching copies of itself to other software in the system. Most viruses are highly destructive. They can lead to outright wreckage of the computer system and a few of them are mere irritants. Trojan horse is related to the computer virus. Though it does no replication of any sort, it is a software that conceals within software. It performs some undesired yet unintended action while, or in addition to pretending to do something else. Some of them fake login programs: an attempt to collect account and password information like a normal login program from the unsuspecting client for a fraudulent purpose (Delger, 1999). Worms on the other hand are self replicating viruses that replicate over a computer network with the ultimate intent of destroying the system or steal the user's identity. With the popularity of the Internet as a veritable tool for e-commerce, the developers have equally increased their intention from system crash to identity theft for the purpose of material or financial gain.

The design philosophies of these malicious programs include: stealth, social engineering, e-mailers, polymorphism armoring and macro (Kubitz).

- Stealth involves an attempt to conceal their presence thus making them difficult to trace.
- Social engineering involves an attempt to gain access to other people's system via a social means, pretending to be a bonafide user or administrator and having the intention of perpetrating identity theft.
- E-mailers have the capability to mail copies of the virus enmass within a short period of time to several hosts around the world. It propagates through MS Exchange server and MS Outlook.
- Polymorphism entails the capability of the virus to exist in more than one form thus having no unique pattern and making its presence difficult to detect.
- Macro features are directed towards the MS office documents that saves macro code within the body of the document.
- Amoring feature entails having special codes that disable antivirus.

Name	Type	Feature	Propagation/effect
Brain Virus	Virus	Stealth	Hides in memory to attack files
Lion worm	Worm	Stealth	Attacks antivirus
Happy99/ska	Worm/Trojan	Social engineering	E-mails copies through attachment
I love you	Worm	Social Engineering	e-mails/copies through attachment
Pathogenic virus	Virus	Polymorphic	Infects DOS files
Queeg virus	Virus	Polymorphic	Infect DOS files
Klez/Bugbear	Worm	Amoring	Disables antivirus
Fizzar/Iirva	Worm	Amoring	Disable antivirus
Code red	Trojan	Keyloggers/password-stealer	Installs denial of service (DOS) agents/backdoors
Fizzer worm	Trojan	Keyloggers/password-stealer	e-mails password and other information to criminals
Osama Bin Laden	Trojan	Social Engineering	E-mails copies through attachment

Table 1. List of Common Viruses, Worms, and Trojan Horses

2.3 CYBER-TERRORISM

Cyber-terrorism is defined as a criminal act perpetrated by the use of computers and telecommunications gadgets, resulting in violence destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to particular political, social or ideological agenda (Elmusharaf, 2004). It is equally considered as the use of computer network tools to shut down critical infrastructure such as energy, transportation and government operations or to coerce or intimidate a government or civilian population.

Another form of cyber-terrorism is perpetrating extortion through the Internet where criminals may lockup useful applications on the system or threaten to shut down businesses with a barrage of data thus leading to a denial-of-service attack if their demands are not met (Srinivasan, 2005). Similarly the web is considered a "web of terror" that is now being used to prosecute electronic jihad (Coll, 2005).

The effects of cyber-terrorism are diverse, ranging from hacking into a web-based IT, to taking a power grid offline, resulting in total blackout; disabling a country's military defense; destroying the economy of a nation through attacks on the basic infrastructure like power, water supply and telephone.

2.3.1 TERRORIST GROUPS

Al-Qaeda has remained the most dangerous terrorist group and an enemy of America following the September 11 attack (Elmusharaf, 2004). Information recovered

from this group has shown that they have ample data on the America's critical infrastructure such as power, telecommunications and water distribution. Al Qaeda uses email and website in Turkey, Nigeria and regions occupied by Pakistan tribes to extend its network (Vladimir, 2004). Other groups are the Unix Security Guards (USG), the World's Fantabulas Defacers (WFD), and the Anti India Crew (AIC).

2.3.2 FORMS OF CYBER TERRORISM ATTACK.

While the financial institutions are the preferred targets for financial gains, other forms are:

a. An attack on NASA, Navy and the department of defense computer system in the year 1998.
b. An attack on Australia waste management control system that released millions of gallons of raw sewage on the town in year 2000.
c. Hackers took control of the computer system that controls the flow of natural gas in Russia in year 2000.
d. In the year 2002, the Israeli Cyber warfare professionals launched attacks disrupting harassing hundreds of computer users and annoying thousands more.

2.3.3 PROSPECTS OF CYBER ATTACK

a. It is cheaper than the traditional approach.
b. Their actions are very difficult to trace.
c. Their identities and location are concealed.
d. There is no physical barrier to prevent their action.
e. The attack is launched remotely and enjoys a wider coverage.
f. Several targets can be hit simultaneously.

3.0 ECONOMICS OF CYBERCRIME

Resent research has shown that the direct economic damages inflicted by cyber-crime is virtually at par with the benefits of IT in business let alone the other social and moral consequences (Vasili, 2003). The author equally put the overall income from cyber-crime in US at $500million in 2000 which would be a lot more by now. While in Germany it was estimated at 70 billion DM a year. A total of $233 billion was realized through e-commerce in the year 2000 and an estimate of $6.8 trillion by the year 2004 (Andrew, 2004). With this huge turnover on the Internet, a Distributed Denial of Service (DDoS) attack on the root servers that powers the Internet communications is of great consequences. The cost of internet down-time for one day is estimated at $6.5 billion (Elmusharaf, 2004). According to FBI estimate in 2004, the cost of cyber-crime is put at $400 billion. The report found that only 5% of cyber-criminals are ever caught or convicted; the use of pseudonyms or online identities provides anonymity that is attractive to fraudsters.

The above estimate of the cost of cyber-crime is highly conservative as most crimes are not reported for fear of corporate reputation.

4.0 EFFECTS ON E-BANKING

Cyber-crimes have grievous consequences on business in general. Regardless of the type of business transaction: e-banking, e commerce and e-government, the major concern is having an efficient payment system (e-payment). With e-payment, the bank is a prime player through e banking facilities. The various problems revolve around identity theft, extortion, phishing, pharming, virus and worm attacks etc. considering the volume of transactions taking place on the web and the amount of money involved, more is desired in the area of trust, confidentiality, integrity, authentication and authorization. Any business that cannot guarantee all these is doom.

5.0 SECURITY MEASURES

Security measures against e-fraud are a horrendous task. The crimes are numerous and perpetrated through diverse means. Therefore an effective security measure would require a fortified approach that would prevent some as there may not be a complete solution. The preventive measure can be discussed under the following headings:

a. Public key Infrastructure (PKI)
b. Intrusion detection and prevention through firewall.
c. Anti-virus, spam, scam, spyware etc.

a. Public Key Infrastructure (PKI)

This approach is aimed at providing digital certificates for web servers through which users/systems can be authenticated, as well as enforcing confidentiality and maintaining data integrity through encryption.

There are quite a lot of public key cryptographic systems available ranging from symmetric, asymmetric and a hybrid of the two. They provide a means by which communication can take place in the presence of possible fraudsters through encryption without being tampered with. Hence the problems of privacy, security and confidentiality are adequately catered for with this. The strength of key depends on the number of bits which range from 40 to 128 bits. The 128 bits is the strongest cryptographic key and takes more than 1 trillion years to crack[1].

In addition, Digital Certificate (CA) provides a means of identifying individuals and websites on the Internet. A "trusted third party" or 'CA' such as VeriSign signs (digital signature) the certificate which is a symbol of security, integrity and confidentiality.

Popular CAs are: i. VeriSign ii. eTrust

b. Intrusion detection and prevention through firewall

Generally, firewalls are barriers to fire and intended to slow down its spread. In the field of IT, the function is not different. It provides a single point between two or more networks where all traffic must pass (check point); where traffic is controlled and authenticated. It serves as a barrier between 'us' and 'them'. They act as a controlled gateway between two or more networks through which all traffic must pass, thus enforcing security policy and maintaining audit trail. It can be either hardware-based or software-based.

Firewalls also act as content screening devices, thus, they are able to scan virus, screen web addresses, scan keywords and report situations. Firewalls can be employed to enforce corporate security policies for the organization.

[1] VeriSign: Building an E-commerce Trust Infrastructure. SSL server certificates and online payment services. *Technical Brief.*

c. Anti-Virus, Anti-Spam, Anti-Spyware etc.

Most of the virus infections are perpetrated through e-mail. But the most daunting is through spam. Spam are unsolicited mails popularly called junks. Thus, there cannot be too much protection on your system, rather, there is need for regular updates to curb the vices.

Below are some products that offer protection against the menace:

S/N	Product	Company	Antivirus	Antispyware	Antispam	Antiphish	Firewall	Privacy	Cost	
									$	₦
1	Total Security Bundle (Ez Armor/ Pestpatrol)	Computer Associates International (Etrust)	√	√			√		70	9,800.00
2	Mcafee Internet Security 2005 7.0	Mcafee	√		√		√	√	65	9,100.00
3	Zone Labs Zone Alarm Security Suite 2005	Encore Software	√		√	√	√	√	63	8,820.00
4	Norton Internet Security 2005	Symantec	√		√		√	√	63	8,820.00
5	PC-Cillin Internet Security 2005	Trend Micro	√	√	√		√		33	4,620.00

Table 2. List of Security Products by cost and area of strength

6.0 RECOMMENDATIONS

There is no complete protection against the problems of cybercrimes, rather a combination of measures are taken to safeguard the system from attack. In the past anti-virus toolkits are known just for detection and removal of virus. With the magnitude of businesses taking place on the Internet fraudsters have resorted to the idea of identity theft: where the personal information of users are copied or stolen. Therefore a useful toolkit must provide solution for spam, spyware, phishing, pharming, virus and worm as well as detecting and preventing intrussion.
Therefore to provide a complete solution for e-payment a robust system is required to guarantee security, integrity and confidentiality.

Below are some useful tips for safe operation:

1. Banks will never ask for account information by e-mail. Beware!
2. Never give computer passwords out on the phone
3. Resist any curiosity regarding request for personal/financial information on the Internet.
4. Check with Better Business Bureau (BBB.org) and scambuster.com before making a purchase from an unfamiliar websites or company.
5. Always resist force-seller tactics when buying goods online.
6. Upgrade the operating system -- Windows XP users should enable automatic updates and install Service Pack 2. Mac users should update with the Software Update Control Panel.
7. Use a firewall. Windows XP has one built-in and a router most likely has one built-in.
8. Adjust browser security settings to medium or higher.
9. Consider an ISP or e-mail provider that offers security.
10. Use antivirus software.
11. Use more than one antispyware program, which can boost coverage.
12. Regularly back-up personal files which safeguards data in case of a security problem.
13. Beware while browsing. Be wary of ad-sponsored or "free" giveaways. They probably include spyware.
14. Avoid short passwords to foil password-cracking software.
15. Use e-mail cautiously -- never open an attachment unless you were expecting it.
16. Use multiple e-mail addresses so you can drop one when it attracts too much spam.
17. Take a stand - don't buy anything promoted in a spam message.
18. Look for secure Websites that show an icon of an unbroken key or a lock that's closed at the bottom of the page. Also the Web address should begin with "https:" when entering personal data.

7.0 CONCLUSION

It is obvious that information theft is the most damaging category of Internet crime, while viruses have been the most costly to business. In all these, only the bank bears the brunt particularly for issues bothering on credit card fraud through identity theft. The global connectivity and anonymity of the internet is responsible for the upsurge in cyber-crimes and perpetrators have over 90% chances of going scott free. Therefore, there is genuine risks that without an assurance of security, a

significant proportion of customers are getting wary of Internet business.

However, to minimize the threat to e-business, companies need a proactive policy at email gateway which blocks unwanted attachments to the organization as well running up-to-date antivirus software, firewalls and install latest security patches. Table 2 provides information on the security measures, the products and the cost implication. There is obviously no product that offers all the needed security, therefore a multiple product is recommended.

REFERENCES

Andrew B. (2004): Legal aspects of e-commerce, [online], computer crime research centre, http://www.crime-research.org/articles/Belousov.asp/.

Babu M. (2004): "What is cybercrime", [online], www.crime-rsearch.org/

Coll. et al (2005): Terrorists turn to the web as base of operation, [online], www.crime-research.org/articles/terrorists_turn/

David Guerin (2003): Fraud in Electronic payment, [online], www.trintech.com

Delger H. (1999): "Computer Virus Help", [online], www.winpro.com

Dmitri K. (2004): German banks experience a sudden upsurge of computer crime, [online], http://www.crime-research.org/news/31.07.2004/532

Elmusharaf M.M. (2004): The new kind of terrorism, [online], Computer crime research centre, http://www.crime-research.org/articles/cyber_terrorism_new_kind_terrorism/

Gould J. (2004): Internet security and fraud: The wild, wild west online, [online], http://www.computer-crime.org

Kubitz Shari: Virus hoax or the real thing: How to tell the difference, www.irdc.pitt.edu/news/articles/

Smith R. (2004): IT expert warns of cyber crime threat, [online], Computer crime research centre, http://www.crime-research.org/articles/2004

Srinivasan (2005): Combatting cyberterrorism, [online], http://www.crime-research.org/analytics/cyberterorism/

Vasili polivanyuk (2003): Cybercrime criminological research, [online], Computer crime research centre, http://www.crime-research.org/

Vladimir Goluber (2003): Plastic cards in Ukraine-fraud classification, [online], Computer crime research centre, http://www.crime-research.org/articles/Goluber august/

Vladimir Goluber (2004): Cyberterrorism: terrorism of the 21st century, Computer crime research centre, http://www.crime-research.org/