Internet Banking With Reference To Cyber Crime: A Mini Review

Manjit Wadhwa

Abstract- While consumer banking accounts are covered under Federal Reserve Regulation E (12 C.F.R. Part 205), which requires banks to provide reimbursement for certain fraud losses, Regulation E does not apply to business accounts. Instead, business and commercial bank accounts are covered by the Uniform Commercial Code (UCC)(1)

Introduction

Under the UCC, business account holders have shorter reporting timelines, less protections, and significantly higher liability for fraud than consumer banking customers. Additionally, individual banks can elect to shorten the fraud reporting timelines even further, or even disclaim certain obligations altogether, through amendments to their commercial banking agreements.1

In short, this means much of the responsibility for protection of your business bank account from cyber crime and other fraud rests squarely on you and your business. This responsibility, and liability, particularly extends to safeguarding against ACH and wire transfer fraud, check fraud, account takeover, and protecting your business' banking credentials.(2,3)

Discussion

Internet connected activities are as vulnerable to crime and can lead to victimization as effectively as common physical crimes. The types of crimes that are currently occurring have existed long before the Internet was around. By virtue of the tools being used today to commit cybercrimes, criminals are now more anonymous and provided with a virtual market of available victims. The responsibility falls on individuals to protect themselves and their families through safe online practices. Non-delivery payment/ merchandise—14.4 percent of the sellers/purchasers did not receive payment/merchandise. 2. FBI-related scams—13.2 percent of criminals pose as the FBI to defraud victims. 3. Identity Theft—9.8 percent were unauthorized use of personal identifying information to commit crimes. 4. Computer crimes—9.1 percent were crimes that target a computer or were facilitated by a computer. 5. Miscellaneous fraud—8.6 percent of scams and fraud included sweepstakes and workfrom-home scams. 6. Advance fee fraud—7.6 percent were the Nigerian letter scam. 7. Spam—6.9 percent of users received unsolicited, mass produced bulk messages. 8. Auction fraud—5.9 percent was fraudulent or misleading information in the context of an online auction site. 9. Credit card fraud—5.3 percent was fraudulent charging of goods and/or services to a victim's account. 10. Overpayment fraud—5.3 percent of victims deposited bad (4,5)

Results

Reviewing credit card and bank statements regularly will often reduce the impact of identity theft and credit fraud by discovering the problem shortly after the data has been stolen or when the first use of the information is attempted. Credit card protection services can often alert a person when there is unusual activity occurring on his or her account, for example, purchases in a geographically distant location or a high volume of purchases. These alerts should not be taken lightly and could be the first indicator that a victim receives that something is wrong. If it seems too good to be true, it is—No one is going to receive a

large sum of money from a dead Nigerian politician, win a huge lottery from being "randomly selected from a database of email addresses," or make big money from "passive residual income a few hours each day working out of your home."(6,7) Many of these crimes go unreported because the victim is too embarrassed to admit to law enforcement that they were duped. Turn off your computer—With the growth of high-speed Internet connections, many opt to leave their computers on and ready for action. The downside is that being "always on" renders computers more susceptible. Beyond firewall protection, which is designed to fend off unwanted attacks, turning the computer off effectively severs an attacker's connection—be it spyware or a botnet that employs your computer's resources to reach out to other unwitting users. (8,9)

Head-global Treasury & A. G. M.

National Bank Of Oman

References

1. Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing. Jump up^
2. Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 0-201-70719-5.
3. ^ Jump up to:a b * Halder, D., & Jaishankar, K. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9 Jump up^
4. Steve Morgan (January 17, 2016). "Cyber Crime Costs Projected To Reach $2 Trillion by 2019". Forbes. Retrieved September 22, 2016. Jump up^ "Cyber crime costs global economy $445 billion a year: report"
5. Reuters. 2014-06-09. Retrieved 2014-06-17. Jump up^ "Sex, Lies and Cybercrime Surveys"
6. (PDF). Microsoft. 2011-06-15. Retrieved 2015-03-11. Jump up^ —"#Cybercrime what are the costs to victims - North Denver News"
7. North Denver News. Retrieved 16 May 2015. Jump up^ "Cybercrime will Cost Businesses Over $2 Trillion by 2019"
8. (Press release). Juniper Research. Retrieved May 21, 2016. Jump up^ "Cybercriminals Need Shopping Money in 2017, Too! - SentinelOne"
9. sentinelone.com. Retrieved 2017-03-24.