WILLIAMS MULLEN
WILLIAMSMULLEN.COM

Cyber-Fraud: Don't Be the Next Victim

09.01.2010
09.01.2010

Let's face it - we live in a digital world where electronic and online transactions are a part of our everyday lives. Companies are under constant competitive pressure to provide faster and more convenient ways for their customers to conduct business electronically. Unfortunately, electronic and online transactions are still vulnerable to security breaches. Despite determined efforts by businesses, Internet service providers, software providers, law enforcement agencies, and individual consumers to make online transactions more secure, private individuals and public companies continue to be victimized by cyber-crimes.

Common cyber-crimes include cyber-extortion, cyber-fraud, and identity theft, with each carried out in a myriad of ways. A well-known tactic used to carry out all three of these cyber-crimes is spamming. Spam emails can be used to obtain unauthorized access to accounts and can deploy massive amounts of malware in the form of computer viruses, worms, Trojan horses, and other malicious software. With enough identifying information about an individual, a criminal can take over that individual's identity to commit a wide range of crimes, such as false applications for loans and credit cards, fraudulent withdrawals from bank accounts, and fraudulent use of telephone calling cards. If the criminal takes steps to ensure that bills for the falsely obtained credit cards or bank statements showing the unauthorized withdrawals are sent to an address other than the victim's, the victim may not become aware of what is happening until the criminal has already inflicted substantial damage on the victim's assets, credit, and reputation.

Spam is increasingly used to target online investors and spread false information about a company. In this way, the fraud is simultaneously perpetrated against the individual investor and the unsuspecting company. To prevent becoming a victim of spam, an investor should never rely solely on an online newsletter or bulletin board posting about an unknown company and should always check that the company files regular reports with the SEC. Similarly, a company should perform regular searches to uncover the fraudulent information circulated about it by spammers.

Identity theft and fraud can be coupled with cyber-extortion, which adds a demand for money to avert or stop the cyber-crime. Cyber-extortion is commonly perpetrated through denial of service attacks and ransomware, which is used to encrypt the victim's data. The cyber-extortionist then demands money for the decryption key. As use of the Internet has become vital to the business operations of many companies, the opportunities for cyber-extortionist have increased. Cyberextortionists typically operate from countries other than those of their victims and use anonymous accounts and fake email addresses. This makes cyber-extortion particularly dangerous because the probability of identification, arrest, and prosecution of cyber-criminals is low. Thus, prevention is should be the focus in combating cyber-extortion.

From a business perspective, a company whose data have been compromised may face significant legal and business consequences: liability to exposed customers, downstream liability to other companies attacked by hijacked information systems, and damage to professional reputation, to name a few. Therefore, businesses should not wait for an attack and then seek justice. Instead, businesses should continually strive to raise their awareness of cyber-security risks and prevention tactics.

The first step in preventing a cyber-attack is being cognizant of the risks. In light of the evolving dangers posed by cyber-threats, businesses must respond with equal force and flexibility. Only employees who require access to confidential information should have it, and those employees should be thoroughly screened, trained, and supervised. A strict firewall policy should be in place to block access to former employees, and - despite the expense - companies should establish extensive monitoring systems and incident response teams to deal immediately with security breaches. Companies should also take advantage of cost-free options made available by Internet service providers, such as free security updates and malware removal tools. In addition, and of utmost importance, companies should familiarize themselves with state and federal regulations affecting their businesses and cyber-security, principally the Computer Fraud and Abuse Act.

Cyber-attack prevention is a moving target, and while the issues and best practices discussed here may serve as a starting point, this article scarcely skims the surface of cyber-crime's complexity. The Federal Bureau of Investigation and the U.S. Securities and Exchange Commission maintain up-to-date websites dedicated to awareness and avoidance of cyber-fraud.

Those resources can be found, respectively, at: http://www.sec.gov/investor/pubs/cyberfraud.htm and http://www.fbi.gov/cyberinvest/escams.htm.

For more information about this topic, please contact the author at 804.420.6446 or bperrow@williamsmullen.com or any member of the firm's Financial Services & Real Estate Team.

Editorial inquiries should be directed to John M. Mercer, 804.420.6443 or jmercer@williamsmullen.com. The Williams Mullen Financial Services & Real Estate Quarterly Newsletter is provided as an educational service and is not meant to be and should not be construed as legal advice. Readers with particular needs on specific issues should retain the services of competent counsel.

Related People

- Robert D. Perrow – 804.420.6446 – bperrow@williamsmullen.com

Related Services

- Real Estate