STATEMENT OF GORDON M. SNOW
ASSISTANT DIRECTOR, CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION
BEFORE THE HOUSE JUDICIARY SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

JULY 28, 2010

Good morning, Chairman Scott, Ranking Member Gohmert and Members of the Subcommittee. I appreciate the opportunity to testify before you today regarding the FBI's efforts to combat cyber crime as it relates to social networking sites.

Let me begin by acknowledging that the rapid expansion of the Internet has allowed us to learn, to communicate, and to conduct business in ways that were unimaginable 20 years ago. Still, the same technology, to include the surge in the use of social networking sites over the past two years, has given cyber thieves and child predators new, highly effective avenues to take advantage of unsuspecting users. These cyber criminals are using a variety of schemes to defraud or victimize innocent social networking site users, some of which I would like to highlight today.

Social Engineering

Regardless of the social networking site, users continue to be fooled online by persons claiming to be somebody else. Unlike the physical world, individuals can misrepresent everything about themselves while they communicate online, ranging not only from their names and business affiliations (something that is fairly easy to do in-person as well), but extending as well to their gender, age, and location (identifiers that are far more difficult to fake in-person). Years ago, we called these types of people confidence or "con"-men. Perhaps as a result of today's hi-tech times, con artists are now referred to as being engaged in social engineering. It should come as no surprise to learn that the FBI is investigating classic investment fraud schemes, such as Ponzi schemes, that are now being carried out in virtual worlds. Other con artists are able to conduct Identity Theft crimes by misidentifying themselves on social networking sites and then tricking their victims into giving them their account names and passwords as well as other personally identifiable information.

In addition to Identity Theft crimes, child predators routinely use social networking sites to locate and communicate with future victims and other pedophiles. In at least one publicized case from last year, an individual attempted to extort nude photos of teenage girls after he gained control of their email and social networking accounts. That particular FBI investigation led to an 18 year federal sentence for the offender, reflecting that these crimes are serious and will not be tolerated.

Fraud Schemes

There are a variety of Internet fraud schemes being used by cyber criminals at any given time. By way of example, a recent fraud scheme involves a cyber criminal gaining access to an unsuspecting user’s email account or social networking site. The fraudster, who claims to be the account holder, then sends messages to the user’s friends. In the message, the fraudster states that he is on travel and has been robbed of his credit cards, passport, money, and cell phone; and is in need of money immediately. Without realizing that the message is from a criminal, the friends wire money to an overseas account without validating the claim.

Phishing Scams

Phishing schemes attempt to make Internet users believe that they are receiving e-mail from a trusted source when that is not the case. Phishing attacks on social networking site users come in various formats, including: messages within the social networking site either from strangers or compromised friend accounts; links or videos within a social networking site profile claiming to lead to something harmless that turns out to be harmful; or e-mails sent to users claiming to be from the social networking site itself. Social networking site users fall victim to the schemes due to the higher level of trust typically displayed while using social networking sites. Users often accept into their private sites people that they do not actually know, or sometimes fail altogether to properly set privacy settings on their profile. This gives cyber thieves an advantage when trying to trick their victims through various phishing schemes.

Social networking sites, as well as corporate websites in general, provide criminals with enormous amounts of information to send official looking documents and send them to individual targets who have shown interest in specific subjects. The personal and detailed nature of the information erodes the victim’s sense of caution, leading them to open the malicious email. Such email contains an attachment that contains malicious software designed to provide the email’s sender with control over the victim’s entire computer. Once the malware infection is discovered, it is often too late to protect the data from compromise.

Cyber criminals design advanced malware to act with precision to infect, conceal access, steal or modify data without detection. Coders of advanced malware are patient and have been known to test a network and its users to evaluate defensive responses. Advanced malware may use a "layered" approach to infect and gain elevated privileges on a system. Usually, these types of attacks are bundled with an additional cyber crime tactic, such as social engineering or zero day exploits. In the first phase of a malware infection, a user might receive a spear phishing email that obtains access to the user's information or gains entry into the system under the user's credentials. Once the cyber criminal initiates a connection to the user or system, they can further exploit it using other vectors that may give them deeper access to system resources. In the second phase, the hacker might install a backdoor to establish a persistent presence on the network that can no longer be discovered through the use of anti-virus software or firewalls.

Data Mining

Cyber thieves use data mining on social networking sites as a way to extract sensitive information about their victims. This can be done by criminal actors on either a large or small scale. For example, in a large-scale data mining scheme, a cyber criminal may send out a “getting to know you quiz” to a large list of social networking site users. While the answers to these questions do not appear to be malicious on the surface, they often mimic the same questions that are asked by financial institutions or e-mail account providers when an individual has forgotten their password. Thus, an e-mail address and the answers to the quiz questions can provide the cyber criminal with the tools to enter your bank account, e-mail account, or credit card in order to transfer money or siphon your account. Small-scale data mining may also be easy for cyber criminals if social networking site users have not properly guarded their profile or access to sensitive information. Indeed, some networking applications encourage users to post whether or not they are on vacation, simultaneously letting burglars know when nobody is home.

The Cyber Underground

The impact of cyber crime on individuals and commerce can be substantial, with the consequences ranging from a mere inconvenience to financial ruin. The potential for considerable profits is enticing to young criminals, and has resulted in the creation of a large underground economy known as the cyber underground. The cyber underground is a pervasive market governed by rules and logic that closely mimic those of the legitimate business world, including a unique language, a set of expectations about its members’ conduct, and a system of stratification based on knowledge and skill, activities, and reputation.

One of the ways that cyber criminals communicate within the cyber underground is on website forums. It is on these forums that cyber criminals buy and sell login credentials (such as those for e-mail, social networking sites, or financial accounts); where they buy and sell phishing kits, malicious software, access to botnets; and victim social security numbers, credit cards, and other sensitive information. These criminals are increasingly professionalized, organized, and have unique or specialized skills.

In addition, cyber crime is increasingly transnational in nature, with individuals living in different countries around the world working together on the same schemes. In late 2008, an international hacking ring carried out one of the most complicated and organized computer fraud attacks ever conducted. The crime group used sophisticated hacking techniques to compromise the encryption used to protect data on 44 payroll debit cards, and then provided a network of “cashers” to withdraw more than $9 million from over 2,100 ATMs in at least 280 cities worldwide, including cities in the United States, Russia, Ukraine, Estonia, Italy, Hong Kong, Japan and Canada. The $9 million loss occurred within a span of less than 12 hours. The cyber underground facilitates the exchange of cyber crime services, tools, expertise, and resources, which enables this sort of transnational criminal operation to take place across multiple countries.

Beyond Cyber Crime

Apart from the cyber crime consequences associated with social networking sites, valuable information can be inadvertently exposed by military or government personnel via their social networking site profile. In a recently publicized case, an individual created a fake profile on multiple social networking sites posing as an attractive female intelligence analyst and extended friend requests to government contractors, military and other government personnel. Many of the friend requests were accepted, even though the profile was of a fictitious person. According to press accounts, the deception provided its creator with access to a fair amount of sensitive data, including a picture from a soldier taken on patrol in Afghanistan that contained embedded data identifying his exact location. The person who created the fake social networking sites, when asked what he was trying to prove, responded: "The first thing was the issue of trust and how easily it is given. The second thing was to show how much different information gets leaked out through various networks." He also noted that although some individuals recognized the sites as fake, they had no central place to warn others about the perceived fraud, helping to ensure 300 connections in a month.

This last point is worth expanding upon. Some social networking sites have taken it upon themselves to be model corporate citizens by voluntarily providing functions for users to report acts of abuse. A number of sites have easy to use buttons or links that, with a single click, will send a message to the system administrator alerting them of potentially illegal or abusive content. Unfortunately though, many sites have not followed the lead. Some sites provide users with no ability to report abuse, while others either intentionally or unintentionally discourage reporting by requiring users to complete a series of onerous steps every time they want to report abuse.

FBI Cyber Mission and Strategic Partnerships

The Department of Justice leads the national effort to prosecute cyber crime, and the FBI, in collaboration with other Federal law enforcement agencies, investigates cyber crime. The FBI's cyber crime mission is four-fold: first and foremost, to stop those behind the most serious computer intrusions and the spread of malicious code; second, to identify and thwart online sexual predators who use the Internet to meet and exploit children and to produce, possess, or share child pornography; third, to counteract operations that target U.S. intellectual property, endangering our national security and competitiveness; and fourth, to dismantle national and transnational organized criminal enterprises engaging in Internet fraud. To this end, we have established cyber squads in each of our 56 field offices around the country, with more than 1,000 specially trained agents, analysts, and digital forensic examiners. Still, we can not combat this threat alone.

Some of the best tools in the FBI's arsenal for combating any crime problem are its long-standing partnerships with federal, state, local and international law enforcement agencies, as well as with the private sector and academia. At the federal level, and by Presidential mandate, the FBI leads the National Cyber Investigative Joint Task Force (NCIJTF) as a multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations in order to determine the identity, location, intent, motivation, capabilities, alliances, funding, and methodologies of cyber threat groups and individuals. In doing so, the partners of the NCIJTF support the US Government's full range of options across all elements of national power.

The FBI also partners closely with not-for-profit organizations, including extensive partnerships with the National White Collar Crime Center (NW3C) in establishing the Internet Crime Complaint Center (IC3), the National Cyber-Forensic and Training Alliance (NCFTA), the InfraGard National Members Alliance in establishing InfraGard, the Financial Services Information Sharing & Analysis Center (FS-ISAC), and the National Center for Missing and Exploited Children (NCMEC).

Just one recent example of coordination highlights how effective we are when working within these closely established partnerships. Earlier this year, Romanian police and prosecutors conducted one of Romania's largest police actions ever - an investigation of an organized crime group engaged in Internet fraud. The investigation deployed over 700 law enforcement officers who conducted searches at 103 locations, which led to the arrest of 34 people. Over 600 victims of this Romanian crime ring were US citizens. The success in bringing down this group was based in large part on the strength of our partnership with Romanian law enforcement and our domestic federal, state and local partners. Through extensive coordination by the FBI's Legal Attache (Legat) in Bucharest, the Internet Crime Complaint Center provided the Romanians with over 600 complaints it had compiled from submissions to the www.IC3.gov reporting portal. In addition, and again in close coordination with the FBI's Legat, over 45 FBI field offices assisted in the investigation by conducting interviews to obtain victim statements on Romanian complaint forms, and by obtaining police reports and covering other investigative leads within their divisions.

Working closely with others, sharing information, and leveraging all available resources and expertise, the FBI and its partners have made significant strides in combating cyber crime. Clearly, there is more work to be done, but through a coordinated approach we have become more nimble and responsive in our efforts to bring justice to the most egregious offenders.

Conclusion

Chairman Scott, Ranking Member Gohmert and Members of the Subcommittee, I appreciate the opportunity to come before you today and share the work that the FBI is doing to address the threat posed by cyber criminals in this country and around the globe. I am happy to answer any questions.