Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

October 1, 2009

TECHNIQUES USED BY FRAUDSTERS ON SOCIAL NETWORKING SITES

Fraudsters continue to hijack accounts on social networking sites and spread malicious software by using various techniques. One technique involves the use of spam to promote phishing sites, claiming there has been a violation of the terms of agreement or some other type of issue which needs to be resolved. Other spam entices users to download an application or view a video. Some spam appears to be sent from users' "friends", giving the perception of being legitimate. Once the user responds to the phishing site, downloads the application, or clicks on the video link, their computer, telephone or other digital device becomes infected.

Another technique used by fraudsters involves applications advertised on social networking sites, which appear legitimate; however, some of these applications install malicious code or rogue anti-virus software. Other malicious software gives the fraudsters access to your profile and personal information. These programs will automatically send messages to your "friends" list, instructing them to download the new application too.

Infected users are often unknowingly spreading additional malware by having infected Web sites posted on their Webpage without their knowledge. Friends are then more apt to click on these sites since they appear to be endorsed by their contacts.

Tips on avoiding these tactics:

- Adjust Web site privacy settings. Some networking sites have provided useful options to assist in adjusting these settings to help protect your identity.
- Be selective of your friends. Once selected, your "friends" can access any information marked as "viewable by all friends."
- You can select those who have "limited" access to your profile. This is for those whom you do not wish to give full friend status to or with whom you feel uncomfortable sharing personal information.
- Disable options and then open them one by one such as texting and photo sharing capabilities. Users should consider how they want to use the social networking site. If it is only to keep in touch with people then perhaps it would be better to turn off the extra options which will not be used.
- Be careful what you click on. Just because someone posts a link or video to their "wall" does not mean it is safe.

Those interested in becoming a user of a social networking site and/or current users are recommended to familiarize themselves with the site's policies and procedures before encountering such a problem.

Each social networking site may have different procedures on how to handle a hijacked or infected account; therefore, you may want to reference their help or FAQ page for instructions.

Individuals who experienced such incidents are encouraged to file a complaint at www.IC3.gov reporting the incident.