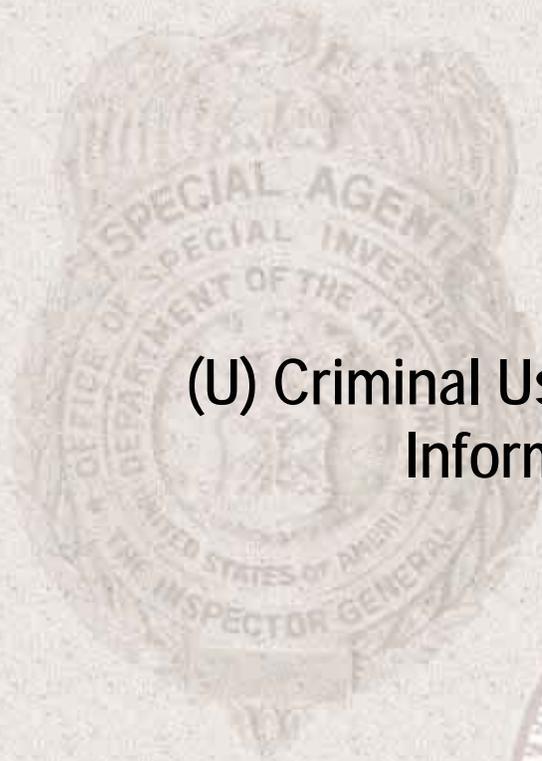




28 Apr 2011

# AFOSI CRIMINAL ANALYSIS SPECIAL PRODUCT

(U) Criminal Use of Military Personal  
Information Online



## (U) Criminal Use of Military Personal Information Online

### (U) INTRODUCTION

(U) The impersonation of military members by scammers using the internet is a growing concern. Scammers use both real and fake military member information to create profiles utilizing social networking sites such as Facebook, dating sites such as Match.com, and online video chat tools such as Skype. Scammers use these profiles to lure victims into trust-based relationships and extort information or money. This report was written to make USAF members aware of this type of activity and inform of techniques to help mitigate the threat.

### (U) DETAILS

(U//FOUO) A “military relationship fraud” is when a victim reports that a person claiming to be part of the military attempts to contact, build a relationship, and scam the victim out of money or information. According to the Internet Crime Complaint Center (IC3), a joint task force established between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C), there were over 130 reported “military relationship fraud” complaints using social networking sites in 2010.<sup>2</sup> This number is on track to increase in 2011.

(U//FOUO) Military Relationship Frauds on Social Networking Sites

	2009	2010	2011 (Projected) <sup>1</sup>
Facebook.com	10	45	~88
Myspace.com	12	25	~4
Match.com	14	25	~52
Other Sites	13	33	~16
TOTAL	49	133	~160

(Figure 1)

(U) Why military members? Online scammers use military members’ information, whether real or fake, for three reasons: (1) credibility, (2) plausibility, and (3) emotional appeal.<sup>3</sup> By appealing to victim’s sensibilities, the criminal establishes trust and loyalty in order to boost credibility once the criminal proposes the scam. The military nexus also gives criminals a credible reason to solicit money from victims that would otherwise make such a request seem suspicious. For instance, a criminal may ask a victim for money in order to fund “visa documents” so that the criminal can “come home from deployment”.

(U) Scammers often use appeals of emotion against vulnerable targets such as older single females. In February 2011, a 53 year-old single Kentucky woman was contacted on Facebook by a person who claimed to be a 26 year-old Army Sergeant. The impersonator used photos from the actual Sergeant’s online public profiles. The impersonator expressed his “undying love” for the woman and asked her for money in order to fund his trip “back home.” In this case, the woman reported the incident to the Army’s Criminal Investigation Command, however, some scammers have taken upwards of \$25,000 from victims.<sup>4</sup>

(U) In 2010, a security researcher created a fake LinkedIn account under the name Robin Sage. The researcher built a prestigious resume for Robin Sage: a degree from MIT, an internship at the National Security Agency, and a current position at the Naval Network Warfare Command (Figure 2). Her address was that of BlackWater, a military contractor. In addition, the researcher included an attractive photograph of a random woman in the profile. Robin Sage gained a total of about 300 friends on LinkedIn. Among the connections were high-level officers in the Joint Chiefs of Staff, the CIO of NSA, an intelligence director for the U.S. Marines, and several DoD and military personnel.<sup>5</sup> The Robin Sage incident highlights how easily even high-level military members are duped into providing personal information to unknown actors.

(U) Robin Sage’s LinkedIn Profile <sup>6</sup>



Summary

I have been in the computer hacking scene for over ten years. During this time I have penetrated hundreds of networks as a professionally contracted hacker and was empowered by the adrenaline rush of breaking into secured facilities of Global 500 companies and various governments. Because of my style and diverse areas of expertise, many of my friends refer to me as the real life Abby Scuito of NCIS.

(Figure 2)

(U) This case highlights the importance of verifying any incoming connection or “friend” requests from unfamiliar profiles. It is best to use another means of communication, such as phone or in-person verification, to make sure the “friend” is a valid connection. Sending a message using the social networking site’s messaging service is not sufficient as the scammer may be aware of personal details that could trick a targeted user into accepting the request. For example, in the Robin Sage incident, when suspicious users questioned the legitimacy of their relationship with Ms. Sage, the scammer messaged back “Don’t you remember, we partied together at Blackhat!” This technique worked against many targets because of their technology background and ambiguity of the answer.

(U//FOUO) In addition to social networking sites, scammers also use online messaging tools, such as Skype, to trick victims. In 2010, a scammer used a high-ranking USAF officer's public online information to create a fake Skype account and contact a victim. The victim became suspicious when the scammer called her using Skype video chat and would not show his face on camera. She also heard suspicious noises in the background which the scammer dismissed as his "military men". The victim herself found the real General's contact information using public online databases and told him about her experience. The General stated that he never opened a Skype account and an investigation took place.<sup>7</sup>

(U) Other incidents where social networking was used to scam victims:

- (U) In March 2009, local authorities in Austin, Texas shut down a Twitter account that impersonated the Austin Police Department. According to open source reporting, the account had hundreds of followers and posted fictitious updates concerning law enforcement activity.<sup>8</sup>
- (U) In January 2009, a fake Twitter profile listed as "The White House" sent out more than 1,500 alerts to over 16,000 followers.<sup>9</sup>
- (U//FOUO) According to the FBI, a malicious actor used information from a government employee's Facebook account to compromise the employee's personal e-mail account. The actor then attempted to extort money from the employee in exchange for not releasing personal information.<sup>10</sup>
- (U//FOUO) In early 2011, scammers spoofed two military Generals using Facebook. The information was pulled from a variety of websites, including the military website with the Generals' listed education, job history, and photographs.<sup>11</sup>

## (U) MITIGATION

(U) The best defense against scammers using information gleaned from military members social networking site profiles is to not have personal information or pictures posted on public websites. Even after the user believes a social networking site profile is deleted, the information may be stored on the host server for years. Data mining websites such as 123people.com comb the web and collect information on users to build entire profiles with publically available information. Users should periodically search for themselves using websites such as Google to not only make sure scammers are not nefariously using personal information, but also to check if data mining websites have built profiles unbeknownst to the user. Many of these sites have an option to remove personal information if you fill out a form or contact their service department.

(U) If using social networking sites, military members should ensure their privacy settings are set so that only trusted connections can read it. Sites such as Facebook and LinkedIn frequently add new features that may disable previous security settings. Therefore, users should often check to ensure their privacy settings are not reset to show personal information to the public.

(U) In addition, posting photos online can sometimes allow scammers to track where and when pictures were taken because of the hidden metadata stored within the digital photograph. This could give scammers detailed information about travel habits and daily activities. A recently released program called “Cree.py” gives nefarious users the ability to use metadata and geocoordinates pulled from posted photographs and user updates on social networking sites to map out exactly where that person has traveled (Figure 3).<sup>12</sup>

(U) Cree.py Mapping Tool



(Figure 3)

(U) Unfortunately, even if a user has not created a social networking profile, the risk is still prevalent because of publically available information. Websites such as radaris.com collect, correlate, and advertise publically available personal information that could be used by a scammer to create a fake profile. Also, the USAF, as well as the other Services, post photographs and personally identifiable information about high-level military officers and civilians on their websites. Adversaries use this information to create fake profiles and exploit unsuspecting victims. If a fake profile is found, users can contact the Internet Crime Complaint Center (IC3) at [www.ic3.gov](http://www.ic3.gov) and report the scam.

## (U) CONCLUSION

(U) Technology has made it easier for online criminals to pose as DoD personnel and lure victims into scams. Users of social networking media should be wary of unknown friend requests and suspicious contact online. In addition, if utilizing social networking sites, DoD personnel should take precautionary steps to ensure that their online data is protected. The best defense against online scammers stealing information is to limit the amount of sensitive data publically available on the internet. As social networking sites gain a larger foothold on the internet and as people become accustomed to divulging personal information such as their daily whereabouts, online scammers will increase their usage of DoD personal information.

---

## REFERENCES

- <sup>1</sup> Projection by Air Force Office of Special Investigation using statistics from January – March 2011
- <sup>2</sup> 2011 Internet Crime Complaint Center, [www.ic3.gov](http://www.ic3.gov)
- <sup>3</sup> Criminal Information Report CIR 10-03: Online Criminals Posing as U.S. Military Personnel, Air Force Office of Special Investigation
- <sup>4</sup> "Con artists impersonate soldiers on Facebook, profess undying love – then ask for cash", Minneapolis Star Tribune, 27 Feb 2011, [www.startribune.com](http://www.startribune.com)
- <sup>5</sup> "Robin Sage Profile Duped Military Intelligence, IT Security Pros", Dark Reading Security, [www.darkreading.com](http://www.darkreading.com)
- <sup>6</sup> "Fake femme fatale shows social networking risks", Computer World, [www.computerworld.com](http://www.computerworld.com)
- <sup>7</sup> Air Force Office of Special Investigation, I2MS Case #19358101940753
- <sup>8</sup> "Twitter Account That Impersonated Austin Police is Shut Down", Dallas Morning News, [www.dallasnews.com](http://www.dallasnews.com)
- <sup>9</sup> "Twitter Says Purported White House Account Was a Fake", Computer World, [www.computerworld.com](http://www.computerworld.com)
- <sup>10</sup> "Cyber Threat: Fraudulent Twitter and Facebook Profiles Impersonating Government-Entities", Federal Bureau of Investigation Intelligence Bulletin, [www.fbi.gov](http://www.fbi.gov)
- <sup>11</sup> Air Force Office of Special Investigation
- <sup>12</sup> "Creepy Stalks Twitter, Flickr Users By Aggregating GPS Data", Gizmodo, [www.gizmodo.com](http://www.gizmodo.com)

## (U) ADMINISTRATIVE INFORMATION

(U) Prepared by: Mark Kuehn, AFOSI Icon Cyber Integration Desk, (240) 857-5362, DSN 857-5362.

(U) AFOSI I2MS Number: DOOP-CI-ANP-33213111251413

(U) All headings without classification markings are unclassified.

(U) AFOSI Threat Products are available on INTELINK-SCI and SIPRNET via the AFOSI Home Pages at [www.afosi.ic.gov](http://www.afosi.ic.gov) and [www.afosi.af.smil.mil](http://www.afosi.af.smil.mil).

(U) Please send your feedback, comments, or suggestions to Mark Kuehn, AFOSI ICON at [mark.kuehn@ogn.af.mil](mailto:mark.kuehn@ogn.af.mil), [mark.kuehn@afosi.af.smil.mil](mailto:mark.kuehn@afosi.af.smil.mil) SIPRNET or [mark.kuehn@afosi.ic.gov](mailto:mark.kuehn@afosi.ic.gov) on JWICS.