



AFOSI SPECIAL PRODUCT



United States: Safeguarding USAF Personnel's Online Presence



Safeguarding USAF Personnel's Online Presence

INFORMATION CUTOFF DATE: 16 Jan 2016

PREDICATION:

This product examines how to protect United States Air Force (USAF) personnel from impersonation, fraud, and possible foreign adversaries online. The intended audience for this product is USAF military members, USAF civilians, USAF employees, and their families. Source documents and analysis within this document were limited to reporting at the UNCLASSIFIED level.

EXECUTIVE SUMMARY

Criminals and foreign adversaries target Department of Defense (DoD) members for two major purposes: fraud and elicitation of sensitive information. Online fraud against USAF personnel has persisted for many years and can take on multiple forms, including romance scams, identity theft, extortion, or a multitude of other scams. Elicitation of USAF personnel by criminals and foreign adversaries is a growing concern, especially as USAF members continue to expand their presence on social networking sites.

Fraudulent online activities involve a wide variety of sophisticated scams and fraud schemes designed to take advantage of the unsuspecting public. Scammers use actual and fictitious information about DoD members in a variety of Internet ploys designed to extort information or money from victims. Even high-ranking DoD civilian and military officials have not been immune to these online schemes, as perpetrators use their identities and photographs to lure and defraud victims. DoD members are particularly susceptible to online impersonation based on their elevated visibility in many social settings and perceived integrity. DoD members' institutional affiliations provide cybercriminals with the reputability and plausibility necessary to make these online scams appear credible; hence, DoD members appear to be attractive targets for Internet imposters because of their personal reputation and the reputation of the institution they represent.

Fictitious online profiles controlled by foreign adversaries have successfully targeted hundreds of DoD members, including USAF personnel. These malicious actors typically create fake profiles on social networking sites with legitimate-looking information and attempt to send "friend" or "connection" requests to unsuspecting victims. Similar to criminal actors, foreign adversaries use photographs and career information posted by actual DoD personnel on social networking sites to create fictitious profiles in order to further entice a victim. Once connected, these malicious actors often attempt to either solicit sensitive information about a victim's career or send private messages with malicious links. DoD members are high-value targets because of their perceived connections to: deployed, garrison, and strategic military operations; the frequent turnover of military personnel; and their access to DoD bases, information, and personnel.

Since the mere act of online impersonation alone may not constitute a crime, the ability for law enforcement authorities to enforce prosecution is limited. Victims of online impersonation should engage directly with the social networking site or application in order to remove the false or offensive information. Typically, impersonations are in violation of the provider's terms of service and the fraudulent profile will be removed.

DoD members should remain vigilant against these types of online activities by reducing their online footprint, securing existing accounts, and reporting any improprieties regarding their personal information or suspicious "connection" requests to appropriate authorities. *Appendix 1* includes instructions on how to remove impersonating information from the most popular social media websites, and *Appendix 2* contains additional steps to help victims of impersonation. Information on what to do if you suspect that you have been a victim of identity theft – to include contacting credit reporting agencies – can be found in *Appendix 3*.

KEY JUDGMENTS

Criminals will continue, into the foreseeable future, to utilize DoD personnel information to target susceptible victims for multiple online fraud schemes, including relationship scams, online sale scams, and advance-fee scams due to DoD member's perceived integrity and elevated social status.

DoD members, including USAF and their families, are high-value targets for foreign adversaries seeking information on DoD operations, bases, personnel, information, and related activities. Therefore, foreign actors will likely continue targeting DoD members, civilians, and their families utilizing social networking sites.

SCAMS TARGETING DoD MEMBERS

The U.S. Federal Trade Commission (FTC), responsible for protecting consumers and promoting trade, suggests that "certain scams are more likely to target the military community, in part because military families may relocate frequently and many service members – for the first time – are living on their own and earning a paycheck."¹ Additionally, military members may be targeted by criminals or foreign adversaries (hereafter, "criminals") for greater access into their social networks, professional associations, or unit affiliations.

The Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) is a unit within the FBI's Cyber Division, "staffed by FBI agents and professional staff employees with expertise in the prevention, detection, and investigation of cybercrime,"² who track reported cases of Internet complaints, with the aim of tracking cybercrime activities, generating leads for law enforcement and intelligence agencies, and publishing public service announcements. The FBI IC3 releases an annual report summarizing fraudulent activity complaints, and has identified some of the following types of crimes as being most prevalent during 2015:³

Victims	Type of Crime	Brief Description and/or Example
67,375	Non-payment / Non-Delivery	“(Non-Payment) Goods and services are shipped, and payment is never rendered. (Non-Delivery) Payment is sent, and goods and services are never received.”
30,855	419/Overpayment	“(419) Solicitations from individuals requesting help in facilitating the transfer of a substantial sum of money. The sender offers a commission or share in the profits, but will first ask that money be sent to pay for some of the costs associated with the transfer. <i>Example: “I am a very wealthy prince from Zendia, but I need your help in reclaiming my funds. I will reward you handsomely for your assistance.”</i> (Overpayment) An individual is sent a payment and instructed to keep a portion of the payment but send the rest on to another individual or business. <i>Example: You want to buy something valued at \$100 from someone. This person wants to send you a \$600 check, and have you send someone else a \$500 check back. – What will happen is that their check will bounce after 1 week, and yours will go through; you lose \$500 + bank fees, and the criminal will not be sending you any item.</i>
21,949	Identity Theft	“Someone steals and uses personal identifying information, like a name or Social Security number, without permission to commit fraud or other crimes, and/or ... perpetrate fraud on existing accounts.” <i>Example: Someone uses your information to obtain a credit card or a loan in your name.</i>
21,510	Auction	“A fraudulent transaction or exchange that occurs in the context of an online auction site.”
19,632	Personal Data Breach	“A security incident involving an individual's sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an unauthorized individual.” <i>Example: Your healthcare provider is hacked, and a criminal steals your information.</i>
18,758	Employment	“An individual believes they are working a legitimate job, and many times end up losing money or laundering money/items, or an individual is solicited about an employment opportunity.” <i>Example: “Earn \$1000/day working from home!!!”-style listings in classifieds ads; Jobs where you end up taking personal liability (such as writing personal checks, or opening bank accounts in your name) for alleged business purposes (“we will pay you back!”)</i>
17,804	Extortion	“Unlawful exaction of money or property through intimidation or undue exercise of authority. It may include threats of physical harm, criminal prosecution, or public exposure.” <i>Example: A 19-year-old female contacts you and the two of you exchange messages over the internet and via cell phone. The two of you exchange sexually explicit photographs. A few days after the photo exchange, an unknown male calls and tells you that he is the female's father and that she is only 16 years old. He demands \$500 to terminate her cell phone contract and buy her a new one or to pay for her therapy related to the incident.”</i>
17,172	Credit Card Fraud	“Credit card fraud is ... theft and fraud committed using a credit card or any similar payment mechanism (ACH, EFT, recurring charge, etc.) as a fraudulent source of funds in a transaction.” <i>Example: Someone uses your credit card information to go on a shopping spree.</i>
16,594	Phishing	“The activity of defrauding an account holder of personal or financial information.”

		<i>Example: A criminal sends you a fake "password reset" e-mail. You fall for the trap, and the criminal uses your username/password to go through your e-mail, find information of interest, and conduct password resets on your other accounts (banking, social media, etc.)</i>
16,445	Advanced Fee	"An individual pays money to someone in anticipation of receiving something of greater value in return, but instead receives significantly less than expected or nothing."
14,812	Harassment / Threats of Violence	"(Harassment) To harass an individual or group. It may include the making of false accusations or statements of fact (as in defamation). (Threats of Violence) An expression of an intention to inflict pain, injury, or punishment, which does not refer to the requirement of payment." <i>Example: You list your job on social media sites as "Bomb Dropper for USAF" - criminals or terrorists scrape your profile, and that of your friends and family, and you begin to receive threats directed at your family.</i>
12,509	Romance Fraud	"An individual believes they are in a relationship (family, friendly, or romantic) and are tricked into sending money, personal and financial information, or items of value to the perpetrator or to launder money or items to assist the perpetrator..." <i>Example: "You are so beautiful, and I am deeply in love with you. (Six days later:) I was robbed, and now I can't get back home, unless you help me. Can you send me \$1,000 for a plane ticket?"</i>
11,832	Government Impersonation	"A government official is impersonated in an attempt to collect money." <i>Example: "This is the IRS, and you owe us money. We are on our way to arrest you right now, unless you send us \$5,000 immediately."</i>
11,562	Real Estate/Rental	"Fraud where property was used to launder money; ... used for counterfeit check schemes or fraudulent cash or virtual currency transactions... Fraud involving a rental. This includes fake rental ads or real ads stolen and advertised by a perpetrator." <i>Example: You pay someone \$1,000/month to rent a home you found online... but the criminal that listed the house for rent, does not own the property, and just stole your money.</i>
<i>All definitions were sourced from the FBI IC3 2015 Annual Report</i>		

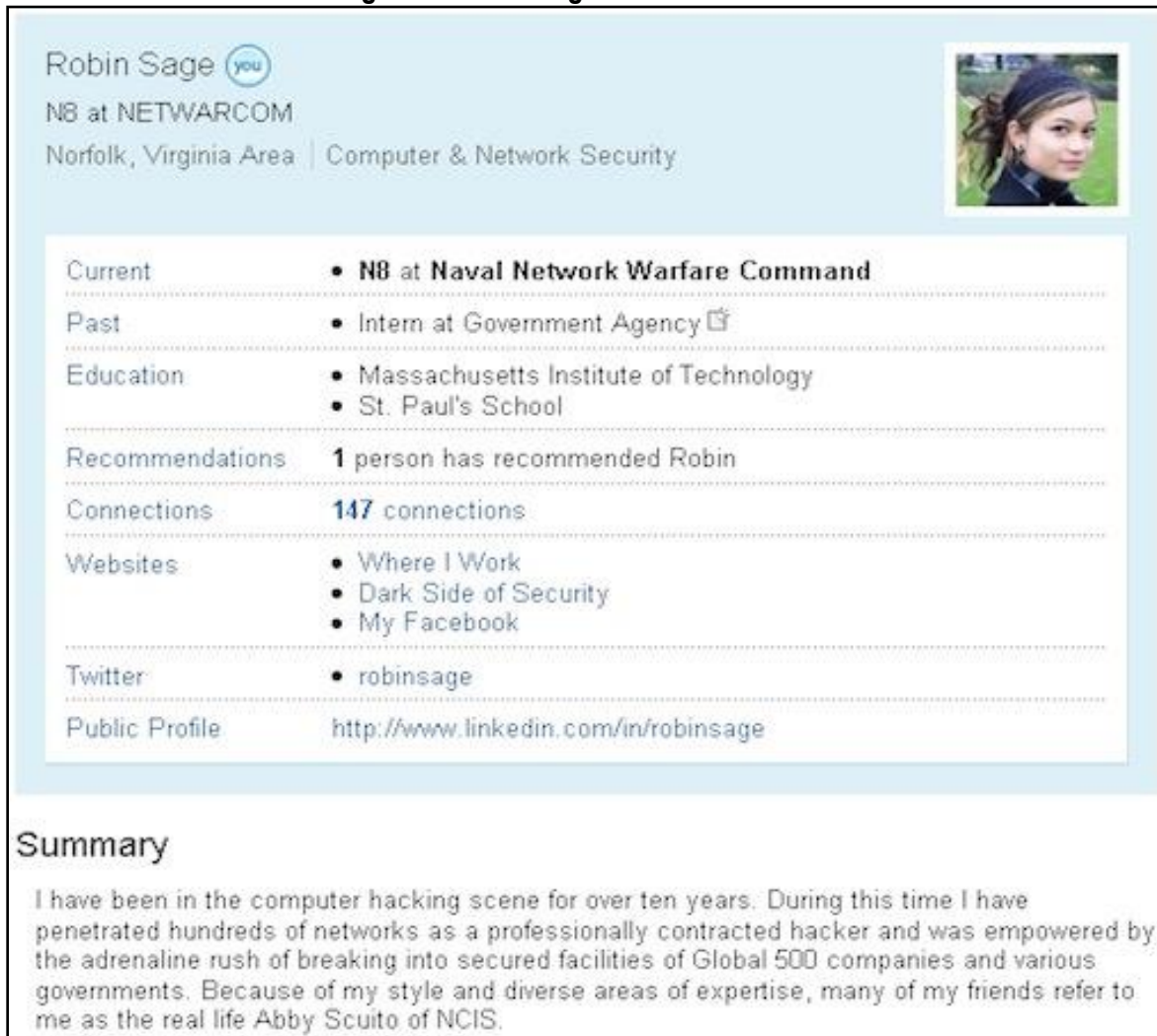
Incidents of Online Impersonation Involving US DoD Members

Recent years have been marked by an increase in online scams involving DoD imposters as cybercriminals looking to exploit the public's confidence in the U.S. armed services. In August 2013, the *Air Force Times* found at least 20 fake profiles impersonating a single senior USAF officer.⁴ Other armed services, including the USAF, are also encountering cases where members have been subjected to online impersonation regardless of rank, thereby confirming that perpetrators are targeting DoD members across services and ranks.

One of the best examples of how susceptible the public is to online DoD impersonation was demonstrated in 2010 when 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 a defense 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 senior DoD and Intelligence Community officials, as well as several other DoD personnel.⁵ The Robin Sage incident highlights how easy it can be to trick even high-level service members into providing personal information to unknown actors.


Figure 2: Robin Sage's LinkedIn Profile ⁶




Robin Sage you

N8 at NETWARCOM

Norfolk, Virginia Area | Computer & Network Security



Current	• N8 at Naval Network Warfare Command
Past	• Intern at Government Agency 
Education	• Massachusetts Institute of Technology • St. Paul's School
Recommendations	1 person has recommended Robin
Connections	147 connections
Websites	• Where I Work • Dark Side of Security • My Facebook
Twitter	• robinsage
Public Profile	http://www.linkedin.com/in/robinsage

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.

Apart from the Robin Sage incident, there are several instances where cybercriminals assumed the identities of high ranking DoD members, including general officers (GOs), in an attempt to scam unwitting victims.

- In 2011, a scammer used a USAF GO's biographical information posted on an AF website to perpetrate an advance-fee online fraud scam. The imposter, claiming to be engaged in a multi-million dollar transfer of Iraqi funds on behalf of U.S. government, attempted to extort personal information from unwitting victims. To further lend credibility to his scam, the perpetrator

hyperlinked to the Air Force's news story depicting the GO's activities in Iraq and interaction with high-level Iraqi military officials.⁷

Scammers utilizing military information often exhibit obvious signs that the profile is fake, including:

- **Lots of “friends” or “connections” added in a short amount of time:** Scammers want to acquire as many contacts as possible to help bolster the legitimacy of their profile.
- **Inconsistencies in profile information, such as suspicious employer or education information:** Scammers will often misspell employers and school names, or may include generic profile information, such as only writing “college” for where they attended school.
- **Sexually provocative profile photo:** Criminals will often use profile photos from actors in pornographic films for their fake accounts. Using these photos allows criminals to gain a substantial following in a short matter of time.
- **Very little profile interaction:** Profiles may include very few or generic comments from the scammer, such as an occasional, “Thanks for the add.”
- **Multiple grammatical errors and spelling mistakes:** Many scammers are not native English speakers and will often phrase information incorrectly or will not capitalize proper nouns, such as their own profile name.
- **Very few real photos:** Scammers will often tag themselves only in cartoons or celebrity photos frequently found on the Internet.
- **Friends are rarely located in the same area:** Since scammers want to connect to as many people as possible, they will spam thousands of users all over the world with “friend” requests; scammers often have very few connections within a local area.

Figure 3: Example of Fake Profile Using Military Information ⁸

The image shows a screenshot of a Facebook profile for 'Sergeant Johnson Mark'. The profile picture is a man in a military uniform with a red beret. The cover photo is a solid blue color. The profile name is 'Sergeant Johnson Mark' with a 'Friend request sent' button. The bio states 'Has worked at Military Channel' and 'Studied at tree hill'. The 'Education and work' section lists 'Military Channel' as an employer and 'tree hill' as a university. The 'Basic Information' section shows the gender as 'Male'. The left sidebar shows navigation options like 'Wall', 'Info', 'Friends', and 'Friends (1)' with a profile picture of 'Janice Dodge Robinson'. At the bottom of the sidebar are options: 'Cancel friend request', 'Share Profile', and 'Report/block this person'.

facebook Search

Sergeant Johnson Mark Friend request sent

Has worked at Military Channel Studied at tree hill

Education and work

Employers **MILITARY** Military Channel

University **tree hill** School year -1

Secondary school **college** School year -1

Basic Information

Gender Male

Wall

Info

Friends

Friends (1)

Janice Dodge Robinson

Cancel friend request

Share Profile

Report/block this person

Foreign Adversaries Targeting DoD Personnel

According to a report by a U.S. information security company, foreign adversaries have targeted over 2,000 people using false personas on multiple social networking sites.⁹ These actors have primarily targeted mid to high-level victims associated with defense contractors and the DoD. Many of these personas are linked to a fictitious news agency, which reposts news articles from legitimate sources, such as the Associated Press and Reuters, and then claims it produced the articles themselves. The report suggests that the targeting originates from Iran.¹⁰ A separate report from a U.S. cybersecurity company identified “28 Chinese adversaries” targeting the Defense and Law Enforcement sectors.¹¹ A third report from a U.S. cybersecurity company suggests Russian government involvement in stealthy computer intrusions targeting U.S. defense contractors.¹² Precise attribution for computer intrusion or targeting is difficult, but the regular identification of this type of activity, and the details within each publication highlights that DoD affiliates are being targeted by foreign adversaries.

Foreign adversaries may be interested in targeting USAF personnel to gain insight into DoD operations, technologies, and personnel. DoD and USAF personnel may be particularly susceptible because of the generally held belief that having a sprawling presence on professional social networking sites, such as LinkedIn, are beneficial to one’s career. Many defense contractors and military associations that work closely with the USAF have their own groups on social networking sites that are open for anyone to join. Many of these groups have thousands of members affiliated with units across the DoD. These groups allow a foreign adversary seeking a target the ability to freely comb through thousands of profiles to find victims of interest, such as those working on sensitive technologies, or DoD members in deployed environments, or members assigned to strategic military missions.

Figure 4: Example of Fake Profile ¹³



Impersonation of USAF Members

According to the International Journal of Cyber Criminology, online fraudsters work to establish credibility and trust with the objective of gaining access to the victim's personal information by associating themselves with highly respected businesses and organizations.¹⁴ By appealing to victims' sensibilities, the criminal establishes trust and loyalty in order to boost credibility once the scam is proposed. The U.S. 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 travel from overseas.

Those who are impersonated online are generally not the victim of criminal activity. The victim is the person scammed out of money, goods, or services and is incurring a loss. While those impersonated may encounter damage to their reputation due to their name's affiliation to the Internet scam, they are not victims of the criminal activity related to the impersonation profile.

Figure 5: Scammers Using Same Public DoD Photo for Multiple Profiles¹⁵



PREVENTION

Although refraining from posting personal information or pictures on public websites is generally the best defense against online impersonators, this is often neither possible nor practical. Nonetheless, US Service members can take proactive measures to reduce their online footprint and mitigate potential risks to their personal information. Outlined below are several measures designed to safeguard personally identifiable information, diminish online presence, and reduce fraud attempts against DoD members or their families.¹⁶

PREVENTION TIP #1: Always practice strong Operations Security (OPSEC) in real life, and online

- **Do not reveal mission-related information** – Do not post sensitive information related to your unit, deployment, activities, or operations tempo, and request that friends and family do the same.
- **Do not use government systems for non-mission-related activities** – Do not use your government e-mail address or phone number to register for non-government affiliated websites.
- **Protect your location** – Do not list your address, military base, unit, or related activities on social networking websites.
- **Use approved means to store or send sensitive information** – Follow department or agency guidelines regarding e-mail encryption. Do not send passwords or sensitive information over e-mail, especially to a non-military (".mil") e-mail address.
- **Do not use personal electronic devices during military missions** – Many mobile applications collect sensitive information (location, audio/video, or network data), even when not in use. Do not bring personal electronic devices during those missions, and keep it safe and secure at home, powered off.

PREVENTION TIP #2: Limit Your Social Network / Internet Presence and Use Caution

- **Only reveal what you would feel comfortable revealing in a public setting** – Use extreme diligence and assume no privacy when posting new information. If a website requires an e-mail address for registration, utilize e-mail services such as Gmail or Outlook.com, to create new accounts, and avoid linking your personal information with these websites. Some services allow for virtual phone numbers, such as Google Voice, and Microsoft Skype.
- **Lock down privacy, access, searching, and sharing settings** – The most popular social networking sites have options for limited exposure of your personal information only to “connections” or “friends” that are explicitly approved by the account owner. Regularly scrutinize the connections to you and your family members, and prune unknown friendships or affiliations.
- **Do not provide information to strangers** – Many trust-based scams begin by the victim answering seemingly benign questions, during irregular periods with strangers online. Over a period of time, criminals or adversaries are able to collect an accurate depiction of you, your unit, your family members, and other related activities, due to clever questioning, and victims providing small but meaningful bits of information during each separate communication.
- **Avoid foreign websites and mobile applications** – U.S. companies must follow U.S. laws and consumer protection guidelines when conducting their business and collecting information. Foreign companies may not be subject to similar consumer protection laws, and foreign governments can exert pressure on technology companies to collect data on DoD members. Before installing an application or registering on a website, determine where that application was developed, where the company is based, and where the servers are hosted. If there is a foreign nexus, consider using a domestic alternative instead, which will provide you with the greatest level of protection.
- **Disable features that automatically broadcasts or tags a photo with your current location** – Cell phones often integrate social media apps directly into the built-in camera application. When a photo is taken, some social media apps will automatically determine your current location and upload that data to your social networking site for all to see.
- **Disable automated GPS and location tracking features when not in use** – Many map and navigation apps on cell phones, tablets, and PCs will continue to collect information about your whereabouts even when you are not actively using them. Carefully scrutinize any applications settings used on mobile devices or home computers as they can be used to determine patterns of life or perhaps tip off your location if used.

-
- **Use discretion when accepting new “friends” or “connections”** – Be wary of accepting invites from names you either vaguely or don’t know and always check directly with a contact before accepting seemingly legitimate requests to join networks or sites.
 - **Limit the personal information you post online** – If possible, do not post your full name, birth date, school information, or work history.
 - **Do not post relationship statuses between you and your significant other, children, or family members** – Such information could be used for targeting purposes by possible criminals.
 - **Do not tag identifiable pictures of yourself online** – If others have posted pictures of you, un-tag yourself. This information could be used to create impersonating profiles or used for targeting purposes.
 - **Permanently deleting your profile is ultimately the best way to prevent information from being collected on you, your friends, and your family.**

PREVENTION TIP #3: Aggregators: Opt Out of Services or Remove the Source of Information

- **Opt out of services of aggregators by visiting their sites and officially requesting that information be removed** – Data aggregators, such as Spokeo.com, Pipl.com, and Intelius.com, collect information on individuals from hundreds of public databases and collates the data onto their website for customers to purchase. This can be done legally without the permission of the individual whose data is collected. Even if a person opts-out of inclusion into the website’s data aggregator, the permission may be reset once the person moves to a new address. Individuals should regularly search for themselves and their families on these websites and opt-out as soon as possible after a move.
- **Limit personal information, such as e-mail addresses, phone numbers, etc., on websites that are searched by aggregators** – In addition to public records, data aggregators collect information from websites associated with social media, online gaming, internet forums, gambling, and hundreds of others. Users should use caution when registering for a website.
- **Delete old accounts, and remove related information** – Delete old e-mail, instant messaging, online forum, and other dated accounts. This will help remove old posts, messages, and other ties to your personal information.

PREVENTION TIP #4: Prevent Fraud

- **Credit Freeze: Prevent anyone from opening a line of credit in your name** – A credit freeze is a free feature from all three credit bureaus, which make it difficult for a criminal to open an account in your name, or to fraudulently obtain your credit report: Learn more: “Federal Trade Commission’s – Credit Freeze FAQ.”¹⁷
- **Accounts: Enable multi-factor authentication** – Many websites and applications are “multi-factor”-enabled (sometimes called “two-factor”); meaning that, aside from a username and password, you need an additional form of verification in order to login. This adds an extra layer of security each time a user logs in. The additional method could be a verification text message, a biometric verification, or a one-time code via telephone. Hundreds of websites support multi-factor authentication, including e-mail providers, financial institutions, and cloud backup providers. **Why?** In the event your username and password are stolen in a data breach, the criminal will not be able to login, because they won’t have your phone, token, or one-time codes. Learn more: at “Lock Down Your Login”¹⁸ and “Two Factor Auth (2FA).”¹⁹
- **Shopping: Buy from legitimate, established vendors** – Avoid online marketplaces without an established presence, avoid unknown foreign sellers, review terms of service closely, and scrutinize all sellers and listings: If it’s too good to be true, it is likely fraudulent.
- **Shopping: Avoid counterfeit or pirated products** – Counterfeit products are frequently of poor quality, and can be unsafe for consumers. Pirated music, movies, and software are frequently accompanied by malicious software, which can infect computers and smartphones with viruses.²⁰

CONCLUSION

Similar to civilian counterparts, DoD members and their families are susceptible to being targeted by criminals conducting fraud and online impersonation activities. Criminals and foreign adversaries looking to impersonate DoD members can find an abundance of personal information from official DoD websites, news articles, and social networking sites, especially on those in high-visibility positions, such as GOs and high-ranking DoD officials. USAF members should be aware that their personal information can be exploited by online imposters and must remain vigilant to protect and minimize their Internet footprint, and avoid becoming the victim of fraudulent activity. USAF members should be equipped with the knowledge of how to recover from online impersonation and identity theft situations.

ADMINISTRATIVE INFORMATION

Product Number: 23926

SOURCE SUMMARY STATEMENT

Original sources of the information contained in this report include reports from The Internet Crime Complaint Center's (IC3) periodic Trend Analysis and Intelligence Brief; and, media and news accounts of online social networking incidents involving service members. The information for this product was derived from open source reporting on global, cyber-criminal activity. AFOSI judges this product to be accurate based on past precedence and the quantity and quality of reporting on this subject matter.

REFERENCES

- ¹ FTC; "Military Consumer Protection"; <http://bit.ly/military-consumer-protection>; accessed 12 Jan 2017.
- ² FBI IC3; "An Investigative Look into the IC3"; <http://bit.ly/2jADUFF>; accessed 12 Jan 2017.
- ³ FBI IC3; "2015 Internet Crime Report"; <http://bit.ly/IC3-2015>; accessed 12 Jan 2017.
- ⁴ Air Force Times; "Online scam impersonates new USAFE commander"; 5 August 2013.
- ⁵ Dark Reading Security; "Robin Sage Profile Duped Military Intelligence, IT Security Pros", Dark Reading Security; 10 July 2010; <http://bit.ly/robin-sage>; accessed 12 Jan 2017.
- ⁶ Computer World; "Fake femme fatale shows social networking risks"; 22 July 2010; <http://bit.ly/cw-robin-sage>; accessed 12 Jan 2017.
- ⁷ Scam of the Day; 8 November 2011; <http://bit.ly/scam-of-the-day>; accessed 12 Jan 2017.
- ⁸ NBC News; "Soldier impersonations target women on Facebook"; 27 Feb 2011; http://www.nbcnews.com/id/41810534/ns/technology_and_science-security/t/soldier-impersonators-target-women-facebook/, accessed 02 Feb 2017.
- ⁹ iSight Partners, "An Iranian Threat Inside Social Media"; Pg. 3; 28 Mar 2014.
- ¹⁰ iSight Partners, "An Iranian Threat Inside Social Media"; Pgs. 10-11; 28 Mar 2014.
- ¹¹ CrowdStrike; "Global Threat Report 2015"; <http://bit.ly/global-threat-report-2015>; accessed 17 Jan 2017.
- ¹² FireEye; "APT28: A window into Russia' Cyber Espionage Operations?"; 27 Oct 2016.
- ¹³ PC World; "Taliban uses sexy Facebook profiles to lure troops into giving away military secrets"; 11 Sep 2012.
- ¹⁴ International Journal of Cyber Criminology (IJCC); Nhan, Kinkade, Burns; ISSN: 0974 – 2891, January - June 2009, Vol 3 (1): 452–475.
- ¹⁵ US Army Public Affairs; "Army stresses caution, education to combat social media scammers"; 11 July 2011; <http://marriedtothearmy.com/are-you-dating-an-army-soldier-or-a-fake/>; accessed 02 Feb 2017.
- ¹⁶ US Air Force public website; "Social Media Guide"; May 2010; <http://www.afpc.af.mil/>; accessed 02 Feb 2017.
- ¹⁷ Federal Trade Commission; "Credit Freeze FAQs"; <http://bit.ly/ftc-credit-freeze>; accessed 13 Jan 2017.
- ¹⁸ National Cyber Security Alliance; "Lock Down Your Login"; <http://bit.ly/lock-down-your-login>; accessed 13 Jan 2017.
- ¹⁹ Josh Davis; "Two-Factor Auth (2FA) - List of Websites and Whether they support 2FA"; <http://bit.ly/twofactorlist>; accessed 17 Jan 2017.
- ²⁰ Department of Homeland Security National Intellectual Property Rights Coordination Center; "Pirated Software May Contain Malware"; <http://bit.ly/iprc-malware>; accessed 13 Jan 2017.

APPENDIX 1: POPULAR SITES

Shortcuts to Report Impersonations on Popular Social Network Sites

Private companies that host social networking or media websites have specific reporting guidelines and contact information for reporting account impersonations. **Account impersonation reporting processes are different for each website, and these processes frequently change over time.** For assistance, please contact the company directly (via their “help” or “contact us” instructions – search for “impersonation” or “report abuse”.)

For your convenience, the contact/report links for the most popular providers are provided below (active as of early 2017):

Social Media Provider	Report Abuse
Apple	http://bit.ly/abuse-apple
Facebook	http://bit.ly/abuse-facebook
Flickr	http://bit.ly/abuse-flickr
Google (Gmail, Google+, ...)	http://bit.ly/abuse-google
Imgur	http://bit.ly/abuse-imgur
Instagram	http://bit.ly/abuse-instagram
LinkedIn	http://bit.ly/abuse-linkedin
MySpace	http://bit.ly/abuse-myspace
Tumblr	http://bit.ly/abuse-tumblr
Twitter	http://bit.ly/abuse-twitter
Yahoo	http://bit.ly/abuse-yahoo

Dating Websites	Report Abuse
Coffee Meets Bagel	http://bit.ly/abuse-cmb
eHarmony	http://bit.ly/abuse-eharmony
Match.com	http://bit.ly/abuse-match
OKCupid	http://bit.ly/abuse-okcupid
Plenty-Of-Fish	http://bit.ly/abuse-pof
Tinder	http://bit.ly/contact-tinder
Zoosk	http://bit.ly/abuse-zoosk

Instructions for other social media or dating websites may be found by conducting an Internet search for “[name of website/app] report abuse” or “[name of website/app] help.” Please only use official resources from the actual website/app provider.

APPENDIX 2: MITIGATION – WHAT TO DO

What To Do If You Have Been Impersonated Online

The owner of the **impersonated** account needs to take action to prevent further/possible criminal activity. Typically, the companies that own and manage the sites do not allow law enforcement or outside entities access to accounts or account owner information. The following actions should be taken immediately:

- **Report the fraudulent account to the website where it is hosted** – This is the fastest and most direct way to remove the impersonating account. For example, if the impersonating account is on Facebook, contact Facebook directly. See Appendix 1 for removal information for popular social media websites, dating websites, and related Internet-enabled applications.
- **Conduct an online search and remove publicly available information** – Often, criminals will use the same impersonated information on multiple social networking or dating websites. A criminal may make multiple profiles with a victim's name, image, or information. Victims should conduct a thorough search to track down fake profiles, and take appropriate steps to remove fake profiles or offending information.
- **Report the incident to the Internet Crime Complaint Center (IC3)** – The victims of Internet crimes should report the impersonation and related activity to the IC3 website at: <http://www.ic3.gov/>. Please describe in detail as much as you can about the impersonation, including if you know that the account was used for scamming victims out of money. The IC3 will include the impersonation and other Internet crimes in its statistics and refer the complaint to appropriate authorities if further investigation is possible.
- **Report this incident to your security officer** – Combatant Commands, Services, Defense Agencies, DoD field activities, and joint and combatant activities (CC/S/A) may have a separate security officer assigned to assist with personnel security and other security matters. Reporting this incident to your security officer helps to keep your CC/S/A aware of threats to your activity, and identify any trends in this activity.

APPENDIX 3: MITIGATION – IDENTITY THEFT

What To Do If Your Information Is Being Used to Commit Fraud or other Crimes

If your information is being used to commit fraud:

- **IdentityTheft.gov** – Use the Federal Trade Commission’s (FTC) **IdentifyTheft.gov**²¹ tool to report this incident, and develop a recovery plan. IdentityTheft.gov is an interactive tool that provides streamlined checklists and sample letters to guide consumers through the process of reporting, reacting, and recovering from identity theft.
- **Report this incident to local police and your security officer** – File a police report. Reporting the incident helps identify trends of criminal activity targeting USAF and DoD members, identify motives, identify additional victims, and direct affected members to resources appropriate to their situation. Combatant Commands, Services, Defense Agencies, DoD field activities, and joint and combatant activities (CC/S/A) may have a separate security officer assigned to assist with personnel security and other security matters. Reporting this incident to your security officer helps to keep your CC/S/A aware of threats to your activity, and identify any trends in this activity.

²¹ FTC; “Identify Theft Recovery Steps”; <https://www.identitytheft.gov>; accessed 16 Jan 2017.