DEPARTMENT OF THE AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS

10 April 2020

Special Product

SUBJECT: Online Impersonation of Service Members

INFORMATION CUTOFF DATE: 31 March 2020

EXECUTIVE SUMMARY

This Department of the Air Force (DAF) Office of Special Investigation (OSI) product highlights the threats posed by cybercriminals who impersonate DAF personnel online. This product also provides mitigation techniques and addresses law enforcement's limited ability to investigate these incidents and remove fraudulent accounts.

IMPERSONATION OF DAF MEMBERS

Cybercriminals frequently impersonate U.S. military member identities to gain trust and confidence of their victims. Once such confidence is gained, cybercriminals increase their chances of successfully defrauding victims due to the added emotional connection and patriotism that is often elicited. These types of scams are commonly referred to as "trust-based relationship scams," to include so-called Romance/Casanova scams in which the criminal uses falsified identities to initiate romantic relationships. To facilitate these types of scams, cybercriminals often impersonate U.S. military members. In 2019, the Federal Trade Commission (FTC) stated that 25,000 consumers filed a report regarding romance scams, totaling losses of over $200 million—up nearly 40% since 2018.[1]

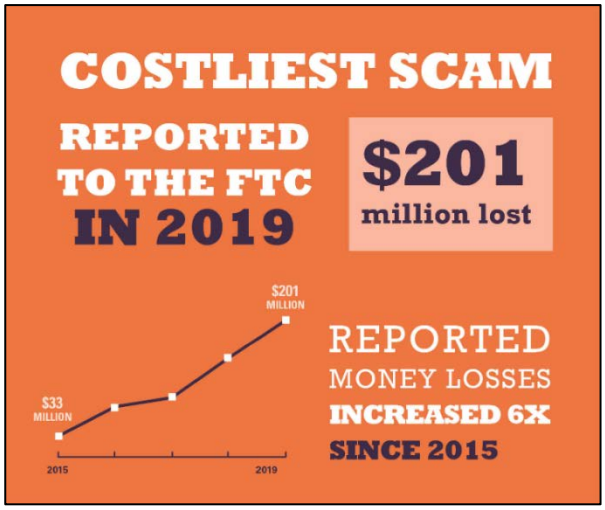

Figure 1: FTC Infographic Depicting Total Dollars Lost to Falsified Identity Scams in 2019

The victims of these scams extend beyond the individuals involved in the fraudulent relationships. The military members, as well as their services, can be negatively impacted by these scams due to reputational loss. The majority of DAF members who have been victims of impersonation have had their photograph(s), and at times their full names or other personal information, used by cybercriminals. While these incidents generally do not directly target DAF members, they can result in law enforcement or victim presumption that the the DAF member actually conducted the scam, leading to possible victim accusation or law enforcement investigation. These activities can also cause potential embarrassment to the member and service.[2, 3]

Mitigating Strategies

Impersonating DAF members can be accomplished using official and personal photos, real DAF member ranks and names, and socially engineered usernames and identifiers (such as military-specific emails and social media handles). Cybercriminals will most likely continue to create false personas using real military member information; however, DAF members can reduce this likelihood by employing some precautionary measures online and exercising proactive vigilance.

Figure 2: USAF Facebook Page Verified Status

OSI recommends performing periodic searches of DAF members' ranks and names across various social media platforms for imposter accounts. Since cybercriminals will use official and personal photos, conducting a reverse image search can help identify imposter accounts. Paid services exist that will identify and report fraudulent accounts, but the actual removal of the account requires the social media platforms (with which the fraudulent account is associated) to review and evaluate the alleged fraudulent profile.

Verified Accounts

DAF members who are considered public figures, such as general officers, senior executives, or public affairs officers, should ensure their social media accounts are verified. A verified account provides a higher degree of legitimacy to that account. These accounts will usually display an icon that indicates the authenticity of the account (e.g. a blue or grey check mark on the account). The verified icon and the process for obtaining a verified account vary depending upon the specific social media platform.[4] Although this does not inherently prevent DAF member information from being used for impersonation purposes, verified accounts can provide potential victims with an indicator that can assist in identifying a fraudulent account.

Reporting Fraudulent Accounts

Nearly every social media site has a feature that allows users to "report," "flag," or otherwise identify fraudulent and impostor accounts. Each site has a different review process, but reporting false accounts to allow for such a review is the most important step in removing fraudulent profiles. Below are removal request links for commonly used social networking and dating websites:

Social Networking/Dating Platform	Removal Request Link
Apple	http://bit.ly/abuse-apple
Facebook	http://bit.ly/abuse-facebook
Flickr	http://bit.ly/abuse-flickr
Reddit	http://www.reddithelp.com
Instagram	http://bit.ly/abuse-instagram
LinkedIn	http://bit.ly/abuse-linkedin
YouTube	http://help.youtube.com
Tumblr	http://bit.ly/abuse-tumblr
Twitter	http://bit.ly/abuse-twitter
Pinterest	http://help.pinterest.com
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

LAW ENFORCEMENT LIMITATIONS

Many trust-based relationship scams do not directly target DAF personnel or resources as the victims of identifiable crimes. As a result, OSI is limited in our ability to investigate such incidents. Additionally, many of these scammers register accounts with fake names, mask their location, and frequently abandon those accounts, further constraining any potential law enforcement response. Law enforcement is also unable to serve as an intermediary between an individual DAF member and a social media service in order to request the removal of fraudulent accounts or profiles. An individual's use of any social media service is based upon a private agreement between the user and service, governed by terms of service. Only the parties to this agreement are permitted to coordinate usage of social media accounts; law enforcement therefore cannot act on behalf of a private user with social media services. If a DAF member believes he or she is the victim of a trust-based relationship scam, OSI recommends reporting the incident to the Internet Crime Complaint Center at https://www.ic3.gov, and reporting the fraudulent account to the respective social media platform.

ADMINISTRATIVE NOTES

Author: OSI ICON Center Cyber Operations Division (ICY); (571) 305-8525
This product was coordinated with: ICON Center Watch Division, Criminal Division, and 3 FIS
Reviewed by: OSI Senior Intelligence Officer

REFERENCES

[1] Internet Site; FTC; New FTC Data Show Consumers Reported Losing More Than $200 Million to Romance Scams in 2019; 12 February 2020; https://www.ftc.gov/news-events/press-releases/2020/02/new-ftc-data-show-consumers-reported-losing-more-200-million; Accessed 31 March 2020.

[2] Internet Site; Vietnam Veterans of America; An Investigation Into Foreign Entities Who Are Targeting Servicemembers and Veterans Online; 17 September 2019; https://vva.org/wp-content/uploads/2019/09/VVA-Investigation.pdf; Accessed 31 March 2020.

[3] Internet Site; Stars and Stripes; Cybercriminals target military online to set up impostor 'romance scams'; 17 September 2019; https://www.stripes.com/cybercriminals-target-military-online-to-set-up-impostor-romance-scams-1.599355; Accessed 31 March 2020.

[4] Internet Site; Search Engine Journal; The Complete Guide to Social Media Account Verification; 6 October 2016; https://www.searchenginejournal.com/the-complete-guide-to-social-media-account-verification/172832/#close; Accessed 31 March 2020.