SNS HARASSMENT AND IMPOSTOR ACCOUNTS

If you are in danger of physical harm, contact the police immediately

Some Internet trolls will use the Internet as a way to threaten or harass other SNS users. If you are threatened with physical harm, you must contact the police immediately and inform your chain of command and AFOSI as soon as possible.

Report the profile as an impostor

Nearly every SNS has a feature that allows you to "report," "flag," or otherwise identify fake/impostor accounts. Every SNS has a different review process but, this is the most important step in getting rid of a fake profile.

Verify your trust relationships

Within a large group of friends, hacker can likely compromise at least one SNS account to forge false trust relationships. Hackers use tactics such as posing as an updated account (e.g. "Sorry, I forgot my password. This is my new account."), or creating fake accounts for real people. One way to verify an SNS account is by contacting the "friend" out-of-band (such as via text message or e-mail) and asking about their current SNS accounts; notify your friend immediately about a suspicious account, and report it using the SNS "report" feature. Remove anyone from your contact lists who you do not know.

Notify your friends and family

Contact your friends and family out-of-band, make them aware of the impostor account, and request that they remove the impostor from any connections, groups, or friendships.

BE VIGILANT | Your online safety begins with YOU!

Common social networking profile and content removal requests links:

Apple: http://bit.ly/abuse-apple
Facebook: http://bit.ly/abuse-facebook
Flicker: http://bit.ly/abuse-flickr
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

Common dating websites profile and content removal requests links:

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

AFOSI

Cybersecurity:

Privacy on Social Networking Sites, Harassment and Impostor Accounts

SIMPLE WAYS TO REDUCE YOUR ONLINE FOOTPRINT

PROTECT YOURSELF

This handout provides simple Social Networking privacy tips that U.S. military members and their families can use to stay safe online.

AFOSI

Increase your privacy settings

Review all settings on your Social Networking Sites (SNS) and ensure they are optimized for privacy. If possible, change your settings to only receive messages from your contacts , to avoid harassment and phishing attempts. If the SNS allows it, increase the privacy settings of all of your previous posts.

Remove or reduce third-party applications

Many applications access information such as your name, contact information, and similar details about your SNS contacts. The data collected by third-party applications is typically not protected in the same way as on the SNS itself, and are often collected under different privacy agreements. By not installing third-party applications, you are reducing the chance that your information can be stolen or used improperly.

Avoid “clickbait”

Avoid “clickbait.” The types of “viral” articles shared on SNS are the same type of articles that attackers attempt to mimic when establishing fake websites to lure in victims. “Clickbait” is a term used for articles that are “sensational or provocative in nature and whose main purpose is to attract attention and draw visitors to a particular web page.”

Delete unused accounts

Many users have SNS accounts created years ago, which remain unused. Those accounts may have weak privacy settings, weak passwords, and personal information that a malicious actor could use to their advantage. Take a moment to locate all of your old SNS or instant messaging profiles/accounts and systematically delete each one.

Avoid “free” WiFi

The security of Internet connections made available at a café or restaurant varies greatly per establishment, and it can be easy for an attacker to setup fake access points to collect personal information from USAF members or infect your computer with malware. Do not connect to WiFi access points without understanding the security risks they pose.

Maintain good Information Assurance (IA) techniques in your home

The same policies and procedures that are used to train DoD members to safely use DoD information systems can be applied to your home computer as well: Do not open e-mail from strangers, keep your software up to date, install antivirus software, lock your computer when not in use, etc.

Assist friends and family members with enhancing privacy settings

Attackers often target victims who are not experts in computer security topics, and use one compromised account to lure in additional victims. By reviewing these topics and best practices with your friends and family, you are increasing the overall “cyber health” of your social network. This makes it more difficult for an attacker to successfully target you, your friends, and family.

Change your password regularly and enable two factor authentication

Don’t use the same password on multiple websites. Two-factor authentication is a security feature that is growing in popularity on many e-mail and SNS platforms. ; Two-factor authentication usually requires a username and password, in addition to acknowledging a text message or e-mail before allowing the user into the website.