This Information Bulletin can be viewed on the Deployment Operations Center Link via the Chicago Police Department Intranet

DOC
Unit 116

01 FEB 2016

2016-INF-051

Crime Control Strategies
Chicago Police Department

INFORMATION BULLETIN

Protecting Yourself—Social Networking & Doxxing

REF: 2014-INF-300

Individuals are currently mining the information that people list on their social networking profiles or accounts to find who they are in the real world. For those of us in law enforcement, this can be especially troubling.

Many social networking websites offer robust personal security customization. If any department member has a social networking profile, they are strongly encouraged to review their personal security settings to ensure that their information is secure. Below are some suggested measures:

- Adjust privacy settings to limit who and what people can view on your profile.
- Be selective of your friends.
- Be careful what links you click on.
- Disable options such as texting and photo sharing.
- Do not post photos of yourself in uniform or other department identifiers.

Doxxing is the Internet-based practice of researching and publishing personally identifiable information about an individual. The methods employed in pursuit of this information include searching publicly available databases and social media websites like Facebook, hacking, and social engineering. It is closely related to cyber-vigilantism, hacktivism and cyber-bullying.

Steps to Protect Yourself from Doxxing:

The following are some of the most commonly targeted pieces of information that can be easily obtained through doxxing:

- Full name
- Age, gender and date of birth
- Location and place of birth
- Email addresses and username
- Phone number
- Social networking profiles, websites and blogs
- Family members' information

It is always a good practice to keep the above bits of information hidden. Even though it is not possible to do this in all cases, you can still take care to protect as much information as you can from going public. You can consider the following additional tips for further protection:

1. Do not upload personal photographs on web albums or photosharing sites such as *Picasa* or *Flickr*. Even if you do, make sure that your album is hidden from public and search engines, and your device gps is disabled.
2. If you do not intend to publicly show your profile on search engines, it is a wise choice to make all the internet profiles private.
3. Maximize the privacy settings of your social network profiles. Make sure that your individual albums and photographs have their privacy settings configured.
4. Do not use the same email address for all you accounts. Instead, create separate email IDs for individual activities such as gaming, forum participation, banking accounts, etc.

Any threats to department members communicated utilizing social networking websites will be fully investigated. Department members should immediately report any implied or direct threats targeting any department member.

Any further dissemination of this document or disclosure of its contents is prohibited without approval of the Chicago Police Department's Deployment Operations Center. Elements of this document may be subject to 28 CFR Part 23. Illinois driver's license or identification images are only for use as authorized by 625 ILCS 5/6-110.1 and 92 Ill. Admin. Code 1020.140. This information shall not be released to the media or general public. FAILURE TO ADHERE TO THESE POLICIES MAY RESULT IN CIVIL, CRIMINAL OR DISCIPLINARY ACTION

Crime Prevention Information Center (CPIC) / (Email) cpic@chicagopolice.org / (P) 312.745.5669 / (Pax) 0100 / (Fax) 312.745.6927

OFFICER SAFETY: ONLINE

REF: 2014-INF-299

Officers should be cognizant when using social media, whether representing the Department or in their personal lives, to protect against potential security breaches.

Police Officer Identification

Identifying oneself as a Chicago Police Officer in a social media arena such as *Facebook* or *Twitter* through photos or text may provide mechanisms for third party applications to identify officers' Personally Identifiable Information.

Privacy Settings

It is recommended that all members ensure that privacy settings are enabled and functioning at the highest level to protect the members' personal information which may be accessed through various social media sites without members' knowledge.

Even enabling social media privacy settings to the highest levels cannot always protect information that a user may not want disclosed. "Back-dooring" is a term that refers to gaining access to a system or information by bypassing the normal authentication and security procedures and mechanisms. This action is commonly taken to access social media site information that is believed to be secure from public disclosure.

Facial Recognition

Internet facial recognition applications exist that have the ability to scrape the internet and link unrelated social media photos and ultimately track them back to members' social media sites.

Smart Phones & GPS

Members should be aware that when uploading photo images or sending messages through a social media site via their mobile phone their exact location when they uploaded the image or text can be determined. GPS location services through mobile phones provide longitude and latitude coordinates of the device when using these applications. Be mindful to deactivate all geolocation data before using these functions on mobile devices.

OFFICER SAFETY: ONLINE

Website Analytics

Website owners have the ability to track and analyze users to their websites. Analytical programs also have the ability to track what websites a user linked to from their site and view users currently online. Analytics provide website owners with the ability to link a member's patterns and activity and make a correlation between personal and professional accounts, especially when using a Chicago Police Department owned computer.

Google is an example of a site that utilizes analytics. *Google* stores and tracks information on every user of its site and members should familiarize themselves with *Google's* terms, privacy and policy use.

Chicago Police Department in Mass Social Media

In light of constant publicity of the Chicago Police Department in mass social media, Members of the Chicago Police Department should take into consideration their public online presence in order to protect themselves and their family members against potential nefarious activities in a cyber environment.

Examples of how easy it is to unknowingly allow personal information to become accessible to third party applications or websites may include:

Signing up for "rewards" or "points" programs - While persons may receive coupons or upcoming sale alerts, it may a cost members their personal information being sent to third party applications or websites which display their personal information publicly.

- A suggested solution can be creating a separate disposable email address solely for junk or unwanted emails.

Applications or Games on social media - Enabling applications, or "apps" on portable devices may pose a risk by unknowingly allowing these apps to gain access to personal information through social media if the user is logged on their account through the user's portable device.

- A suggested solution can be to avoid downloading untrusted applications. Members should make sure to familiarize themselves with the application's privacy policy.

If a member knows there is a potential for personal information that may leak publicly online, a suggested solution can be to create a "Google Alert" on the member's and/or their family members' names.
https://google.com/alerts

DOC
Unit 116

Crime Control Strategies
Chicago Police Department

INFORMATION BULLETIN

This Information Bulletin can be viewed on the Deployment Operations Center Link via the Chicago Police Department Intranet

01 FEB 2016 2016-INF-050

OFFICER SAFETY: ONLINE

Removing Personal Information Online

The following websites provide suggestions and links to various websites that collect and retain personal information and how to "Opt Out" of their databases:

https://inteltechniques.com/hfti.links.html

Opt Out of *Google*

Google Maps Street View
- Locate the image in Street View
- Click "Report a problem" in the bottom-right of the image window.
- Complete the form and click "submit."

Opt Out of Behavorial Advertising

http://www.networkadvertising.org/choices/

Deleting Accounts

Simply deleting a social media account may not delete all information. The following site may assist members who wish to fully delete a social media account:

www.deleteyouraccount.com

Any further dissemination of this document or disclosure of its contents is prohibited without approval of the Chicago Police Department's Deployment Operations Center. Elements of this document may be subject to 28 CFR Part 23. Illinois driver's license or identification images are only for use as authorized by 625 ILCS 5/6-110.1 and 92 Ill. Admin. Code 1020.140. This information shall not be released to the media or general public. FAILURE TO ADHERE TO THESE POLICIES MAY RESULT IN CIVIL, CRIMINAL OR DISCIPLINARY ACTION