Social Networking & Doxxing

Reference

- Crime Prevention Information Center (CPIC) / 2020-INF-0445 / 07 June 2020
- AMC Reference #266207 Social Networking and Doxing (2021-INF-222) 23-Apr-2021 12:22

Contact The Office of Communications

If subject of a doxing incident or have knowledge of one regarding another CPD officer, contact Office of Communications as soon as possible at 312-745-6111 or nwsaffr@chicagopolice.org. The Office of Communications will work as expeditiously as possible to ensure members and their family's safety while you are working tirelessly to serve and protect our city. The Office of Communications will immediately contact the social media site(s) to have the post(s) taken down and will also contact the Office of Legal Affairs.

Social Media Security

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

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 cybervigilantism, hacktivism and cyber-bullying.

Protect Yourself from Doxing

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

- 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 such as “Picasa”. Even if you do, make sure that your album is hidden from public and search engines.
2. If you do not intend to show up 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.
5. Activity on social media such as liking a post or commenting on another individual, group, news post may expose your information. Even though your settings may be set at the maximum privacy setting, the other persons or groups may not be and therefore your information on that post is also public.

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.

Public Records Websites

Public record websites periodically scrape social media networks, archived websites, public records databases, and other sources of potentially useful data points and present their findings online. Information captured by these websites may include names, birth dates, current and/or previous addresses, names of relatives and associates, social media profile photographs, archived social media information, work locations, job titles, salaries, real estate records, telephone numbers,and more. Though these websites can serve legitimate purposes such as aiding law enforcement or employers in background investigations, they are also attractive to threat actors seeking to gather information about targets to use in doxing campaigns or other nefarious activity.

Removing Personal Information Online

The following websites provides links to various public records websites that collect and retain personal information and how to “Opt Out” of their databases:

- archives.com https://www.archives.com/optout
- beenverified.com https://www.beenverified.com/app/optout/search
- cyberbackgroundchecks.com https://www.cyberbackgroundchecks.com/removal
- dobsearch.com https://www.dobsearch.com/people-finder/search-name.php
- familytreenow.com https://www.familytreenow.com/optout
- fastbackgroundcheck.com https://www.familytreenow.com/optout
- fastbackgroundcheck.com https://www.fastbackgroundcheck.com/removal
- fastpeoplesearch.com https://www.fastpeoplesearch.com/removal
- instantcheckmate.com https://www.instantcheckmate.com/opt-out/

- intelius.com https://www1.intelius.com/optout
- peekyou.com https://www.peekyou.com/about/contact/optout/
- peoplefinders.com https://www.peoplefinders.com/opt-out
- privateeye.com https://www.privateeye.com/static/view/optout/
- premium.whitepages.com https://support.whitepages.com/hc/en-us/requests/new
- searchpeoplefree.com https://www.searchpeoplefree.com/opt-out
- spokeo.com https://www.spokeo.com/optout
- spydialer.com https://spydialer.com/Consumers/
- truepeoplesearch.com https://www.truepeoplesearch.com/removal
- truthfinder.com https://www.truthfinder.com/opt-out/
- usa-people-search.com https://www.usa-people-search.com/manage
- whitepages.com https://www.whitepages.com/suppression_requests
- xlek.com https://www.xlek.com/optout.php
- zabasearch.com https://www1.intelius.com/optout