Stone Busailah, LLP
DEFENDING THOSE WHO PROTECT OTHERS

1055 East Colorado Boulevard, Suite 320
Pasadena, California 91106

Tel (626) 683-5600 Fax (626) 683-5656

PRIVACY TIPS FOR PUBLIC SAFETY EMPLOYEES

February 2021

A few years ago, after an LAPD fatal shooting, the officer's private information showed up online, including his home address, phone number, personal details - including his child's school location. "Doxing" is the practice of researching and posting identifiable information about an individual; typically, done with malicious intent. Once law enforcement employees have been exposed through doxing, they may be targeted for online harassment. While you may not be able to have full privacy on the internet, you can make it more difficult for people to find your private information.

Even if you make a conscious decision to avoid social media, it's still advisable to take measures to protect yourself online. As you probably know, a quick search can lead to information about almost anyone - including their address, age, places they have lived and even names of their extended family members. You usually can't prevent someone from posting about you online; whether this happens to be a well-meaning friend, an association you belong to, or someone who may want to harm you.

What you can do to protect yourself:

Profiles: Use a non-identifying profile photo on social media and consider using a fake name or your middle name as your surname. Never post photos of yourself in uniform online, as this makes it easier for those with malicious intent to find you when you're off duty. Even using an image of a badge suggests what you do for a living and can make you a target. Choose something innocuous to use as your profile photo. If what you're thinking of posting assists in identifying you--don't post it. This warning includes posting photos of your pets, vehicles and significant others.

Watch Your Posts: Assume information you share online will not remain on your feed only - pay attention to the information your friends and family share. Consider "untagging" yourself on posts. Even what might appear to be harmless - a photo of you walking your dog, a photo containing an award from work, a photo of your child in front of their school - can give others important clues about your location, and may put you and your family at risk.

Don't Put Out Personal Info: Only supply the bare minimum of information when filling out online (and offline) forms or social media profiles. Criminals may be able to use such details - like your birthday, your hometown, and names of parents or siblings - to answer password reset security questions.

Low-Profile Credit Cards: Your method of payment should not reveal your occupation to every merchant, store or provider of services. Instead, consider having a card with no police-centric branding. For example, The Police Credit Union of California offers a "low profile" version of their credit card and debit card that only has "PCU", and not the full name of the credit union, printed on it.

Search Yourself: Search your name and see what kind of information exists about you. Are you "tagged" in other people's photos? Did you accidently post revealing information? Are there

1055 East Colorado Boulevard, Suite 320
Pasadena, California 91106

Tel (626) 683-5600 Fax (626) 683-5656

articles that mention you? Knowing what's out there, may assist in any clean-up process.

Scrub the Net: There are ways that officers can remove personal information from the dozens of websites that sell your information (e.g., WhitePages, BeenVerified, PeopleFinders, Spokeo). While it may be possible to do this yourself, if you believe this to be necessary for your protection, there are companies that do this specifically for officers - at a cost.

Mail: Consider going paperless for statements or use a post office box as a mailing address. To help keep your street address from getting into the wrong hands, consider using a P.O. Box as your address when filling out any kind of form. While you may need to give a residence address for some public records, you can use a P.O. Box for most other situations. Since criminals still use "old-fashioned" dumpster diving to steal private information, it is important to shred any sensitive documents before throwing them away. Also, try to avoid leaving documents in the mailbox overnight.

Privacy Settings: Tighten the privacy settings for your social media profiles. Limit the people that can see the things you post to a small circle of friends - who you know well. And, never accept friend requests from strangers. It's also wise to log out of Facebook after each use (especially while traveling or accessing your account at different locations) and disable your location settings when using search engines like Google.

Updates: Routinely update your computers, devices, and software with the latest security fixes. Use anti-virus software. Choose unique, strong passwords for each of your accounts and change your passwords regularly. Add protection to your email, social media, and online bank accounts by using two-factor authentication techniques.

Takeaway

The pervasiveness of the internet is now a part of normal everyday life. Since it is not possible to control what other people may post about you, the next best thing is to be as proactive as possible. Simply ignoring what's out there about you on the internet or social media isn't a good tactic; remember the old adage, "if you don't have a seat at the table, you'll be on the menu." **Protect yourselves and your privacy.**

Stay Safe and Healthy!