

Tips to preventing physical and online attacks for doctors

BC's physicians are increasingly facing concerns about safety, both online and in practice. To support members and to address these challenges, a series of two-hour webinars were led by security experts Carl Prophet and Julie Jones who are devoted to helping doctors arm themselves with the information they need to ensure their safety.

The following is a summary of the information shared in the webinar.

Physical safety

Threats to safety can originate from a number of areas, each with a potentially different focus and motivation.

Impulsive attacks are:

- Immediate.
- Reactive.
- In the heat of the moment.

Opportunistic attacks are:

- Usually financially motivated.
- Usually targeting property.
- Usually executed by a drug dependent or professional thief.

Targeted attacks are:

- Specific to the victim.
- Most often motivated by financial reward or revenge.
- Characterized by social engineering, stalking, and violence.

The key to
prevention
is **perception**

Perceiving a threat or assault threat quickly is based on:

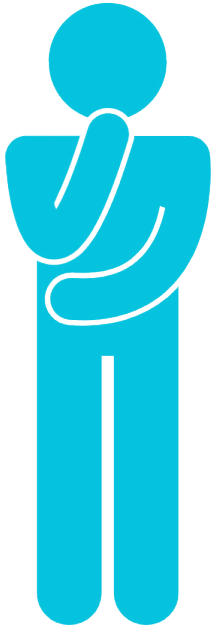
Constant vigilance and situational awareness:

Pay attention to the environment and your experiences.

Predicting the situation:

What does the situation suggest? Look for cues that have the potential to develop into a risk of violence.

Ask yourself these questions before you are faced with the possibility of an attack:



What can I do to prevent attacks at certain times and locations?

Change your route, change the time of day you do certain tasks, etc.

Where and when am I most vulnerable to an attack?

Could be related to a certain time of day, location, routine, or role.

What is the source of the attack?

Determine if an attacker has the intent, means, and opportunity to follow through with an attack.

What can be done to disrupt the threat?

How can you take away the opportunity and means?

Potential signs that are a common precursor to a targeted attack:



Tampering with your vehicle (damaging locks), property (disarming exterior lights), mail or garbage (attempting to gain personal information), or attempts to gain entry into your home or work.



Indications you are being watched in predictable locations at predictable times, such as your work place during work hours, child's school at drop off or pick up, or at your home during dinner time.



Communication designed to locate you or ascertain your schedule (phones calls asking if you are working that day) or online searches of your profile and social network.

Online safety

Preventing an online data breach of your personal information begins with awareness and taking some simple steps to ensure your online privacy.

Tips to keep your security and privacy intact:

- Change passwords every six months at the least.
- Use a password generator to help create strong passwords, or read [this document](#) from the Doctors Technology Office about creating complex passwords that you can easily remember.
- Enable two-factor authentication using services like Google Authenticator, but don't use a phone number as the second factor authentication.
- Do not allow your device to remember your logins and passwords for apps or frequently visited websites.
- Use location services with caution. Location services can be used as a tool to reverse engineer your location and schedule. Some social media apps pull data about your location, which is easily discoverable online.
- Use haveibeenpwned.com to check if your email or phone is involved in a data breach.
- There are many publicly available geo-location and data mining tools on the internet that can easily expose your personal information and location.
- Ensure you know how to set up your social media accounts safely. Read the [social media privacy and security handout](#) for step-by-step instructions on safely setting up privacy and security settings on Facebook, Twitter, LinkedIn, and Instagram.

*“Privacy isn't important until it's **too late.**”*

All information is based on the Human Safety Optimization webinar hosted by Julie Jones and Carl Prophet. This webinar will be offered to Doctors of BC members on an ongoing basis.