# Surveillance

Surveillance is the monitoring of people?s behaviour, activities, or other patterns for the purpose of harming, influencing, managing, directing, or protecting them.

**Why might people be interested in keeping you under physical surveillance?**

* Break-in/ theft of sensitive materials
* Arrest
* Monitor who is coming and going from the office
* Intimidation
* Physical attack on staff

**Who might be interested in keeping you under surveillance?**

* Authorities of the country in which the regional office is located (police, intelligence, military)
* External security agencies of other countries in the region
* Criminals
* Terrorists
* Private contractors
* Embassy officials of ?friendly? countries
* Individuals (may be disgruntled with the organisation)

# What techniques are available to carry out surveillance?

* Digital surveillance (monitoring of digital communications, mobile phones etc.)
* Human surveillance (on foot, in a vehicle)
* Technical surveillance (bugs, listening devices, video cameras, number plate readers etc.)

These lessons deal with how to counter human surveillance. For advice on digital surveillance see the Information and Communications lessons. For advice on how technical surveillance see the Meetings lesson and Home/Office section.

## How to Identify if Your Office is Under Surveillance

Surveillance generally requires that the adversary is able to observe the activities of its targets. This means there are a limited number of physical sites they can use for surveillance. The best thing to do when looking for surveillance is to try to think like an adversary ? what might you do is you were trying to monitor your office? From where might you carry out such surveillance?

* **Take a baseline**  
  It is important to gain an understanding of what ?normal? conditions look like. (For example, where cars normally park or people normally stand).
* **Identify and record**  
  From this, try to identify and record any unusual activities. (For example, people in locations where they shouldn?t be or aren?t normally).
* **Filter out coincidence**  
  Filter out the chances that something could be a coincidence by concentrating on unusual activities and applying common sense filters (e.g. if someone is standing in a place where people don?t normally stand pay more attention to them. Do they look like they are from the area? Are they paying an unusual amount of attention to your activities?) Look for 3 signs that something is out of the ordinary or 3 repeat sightings.
* **Notify others**  
  It is important to notify others of any suspicions and to keep a log of them. This allows the monitoring of patterns which otherwise might not emerge. For example, if you notice someone suspicious and then a colleague notices something else suspicious on a separate occasion but this information is not shared, then a valuable opportunity to confirm a security threat is missed.
* **Trust your senses**  
  Trust your senses ? there may be clues of a potential arrest or violent attack. Often, HRDs report that there were warning signs prior to an attack, but they chose to ignore the warning signs or dismissed it as paranoia.

# What To Do If Your Office Is Under Surveillance

* **Consider the risks**  
  Confrontation with suspicious people should be done with caution, before doing so, consider the risks. For example, what might that person be doing? What is the past history of threats against your organisation or yourself? Is it likely that they will attack you immediately if you confront them or is it more likely that they will just leave and send someone else? If you confront someone they are likely to be replaced by another (unknown) agent, and you then lose the benefit of being able to monitor the surveillance being carried out against you.
* **Increase protection**  
  Increase your office protection by reducing the ability of an adversary to conduct surveillance. For example by putting up screening near your building, using CCTV and/or guards, closing blinds, locking gates, selecting sites which are not easily overlooked, strict access controls to your building etc.
* **Continue monitoring**  
  Continue to monitor the general security environment and increase your observation of threats during periods of higher tension ? e.g. protests, elections, sensitive national holidays etc.

Swipe right for this lesson's checklist

Go to the Advanced Lesson for advice on how to practice counter-surveillance when you are out on foot.

[Go to Advanced Lesson](umbrella://lesson/counter-surveillance/1)

Go to the Expert Lesson for advice on how to practice counter-surveillance when you are out in a vehicle.

[Go to Expert Lesson](umbrella://lesson/counter-surveillance/2)

### RELATED LESSONS/TOOLS

* [Malware lesson](umbrella://lesson/malware)
* [Passwords lesson](umbrella://lesson/passwords)
* [Protecting Files lesson](umbrella://lesson/protecting-files)
* [Making a Call lesson](umbrella://lesson/making-a-call)
* [Sending a Message lesson](umbrella://lesson/sending-a-message)
* [Email lesson](umbrella://lesson/email)
* [Radio lesson](umbrella://lesson/radio)