CONSCIOUSNESS vs. CARELESSNESS

Whether the person, the information, or both are traveling overseas, information electronically transmitted over wires or airwaves is vulnerable to foreign intelligence services' interception and exploitation.

Many countries have sophisticated eavesdropping/ intercept technology and are capable of collecting information we want to protect, especially overseas.

Numerous foreign intelligence services target telephone and fax transmissions. Suspicious entities can easily intercept voice, fax, cellular, data, and video signals.

It is the conscientiousness or carelessness of the individuals responsible that determines whether or not our sensitive information is protected from unauthorized disclosure.

BOTTOM LINE:

BE ASSERTIVE. BE ALERT. BE AWARE.

REPORT SUSPICIOUS ACTIVITY!

SECURITY Countermeasures

Some commonsense security countermeasures should include:

- Do not publicize travel plans and limit sharing of this information to people who need to know
- Conduct pre-travel security briefings
- Maintain control of sensitive information, media, and equipment. Do not pack these types of articles in checked baggage; carry them with you at all times. Do not leave them unattended in hotel rooms or stored in hotel safes
- Keep hotel room doors locked. Note how the room looks when you leave
- Limit sensitive discussions. Public areas are rarely suitable for discussion of sensitive information
- Do not use computer or fax equipment at foreign hotels or business centers for sensitive matters
- Ignore or deflect intrusive or suspect inquiries or conversations about professional or personal matters
- Keep unwanted sensitive material until it can be disposed of securely

Report suspicious activity to your local security contact.
Your DSS point of contact is:

Foreign Travel VULNERABILITY

This product created by Defense Security Service, Counterintelligence Directorate
https://www.dss.mil/isp/count_intell/count_intell.html

FOREIGN TRAVEL

Foreign travel increases the risk of foreign intelligence targeting. You can be the target of a foreign intelligence or security service at any time and any place; however, the possibility of becoming the target of foreign intelligence activities is greater when you travel overseas. The foreign intelligence services have better access to you, and their actions are not restricted within their own country's borders.

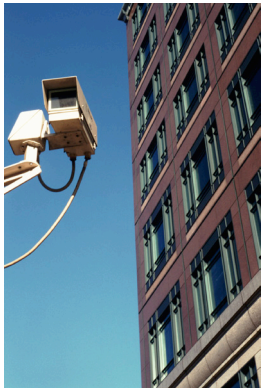
Collection techniques include:

- Bugged hotel rooms or airline cabins
- Intercepts of fax and email transmissions
- Recording of telephone calls/conversations
- Unauthorized access and downloading, including outright theft of hardware and software
- Installation of malicious software
- Intrusions into or searches of hotel rooms, briefcases, luggage, etc.
- Recruitment or substitution of flight attendants

Favorite Tactics

Overseas travelers and the information in their possession are most vulnerable during transit.

Many hotel rooms overseas are under surveillance. In countries with very active intelligence/security services, everything foreign travelers do (including inside the hotel room) may be monitored and recorded.



Entities can analyze their recorded observations for collecting information or exploiting personal vulnerabilities (useful for targeting and possible recruitment approaches).

A favored tactic for industrial spies is to attend trade shows and conferences. This environment allows them to ask questions, including questions that might seem more suspect in a different environment. One assessment estimated that one in fifty people attending such events were there specifically to gather intelligence.

Computer SECURITY

Cleared contractors provide critical research and support to programs giving the United States an economic, technological, and military advantage.

In a world where reliance on technology continues to grow, foreign entities have increased the targeting of electronic devices such as laptops, computers, and personal media such as Personal Digital Assistants and cell phones.

Travelers should report theft, unauthorized or attempted access, damage, and evidence of surreptitious entry of their portable electronics.

The following countermeasures can decrease or prevent the loss of sensitive information:

- Leave unnecessary electronic devices at home
- Use designated "travel laptops" that contain no sensitive information
- Use temporary email addresses not associated with your company
- Perform a comprehensive anti-virus scan on all electronic devices prior to departure and upon return
- Encrypt data, hard drives, and storage devices whenever possible
- Use complex passwords
- Enable login credentials on laptops and other devices