

FBI Omaha Counterintelligence Strategic Partnership Program

December 1, 2010

Counterintelligence Trends

Resources for the Security Professional

Federal Bureau of Investigation

4411 S. 121st Court

Omaha, Nebraska 68137

Executive Management

- **Weysan Dun**, *Special Agent in Charge*
- **James C. Langenberg**, *Asst. Special Agent in Charge, National Security Program*
- **Edward C. Reinhold**, *Asst. Special Agent in Charge, Criminal Program*

Before we jump into the topic for this issue, I would like to introduce Special Agent Mary Dolan, the Omaha Division's new Strategic Partnership Coordinator. Starting December 1, 2010, SA Dolan will be the point of contact for any Strategic Partnership concerns you may have. SA Dolan will also be the new InfraGard Coordinator for the Omaha Chapter. SA Dolan brings many years of diverse experience to both the SPP and InfraGard, and will provide valuable liaison and training opportunities to all of our private and public partners.

Now, on to the main event.....

The recipients of this newsletter represent a diverse group of individuals working for the government, the military, academia, the defense industry, high tech firms, research institutes, and other business and industrial sectors.

What we strive for each month is to put together a product that is educational, informative, and that brings a value added sense to the reader.

Most of the content of our newsletters is information that is publicly available, usually from the internet (with attribution and sourcing). We put this newsletter together as an educational tool, as a resource that

Questions about the Omaha Field Office Counterintelligence Strategic Partnership Program:

Special Agent Mary Dolan, In-Coming Strategic Partnership Coordinator

Cell: 402-250-3389; Email: Mary.Dolan@ic.fbi.gov

that the busy security professional can look to for ideas for training and educational programs within your organizations. And, as always, we use this newsletter as a vehicle to publicize the availability of presentations and vulnerability assessment tools to assist you in your security education programs, and your overall security posture.

First and foremost of these resources is the **InfraGard program**. Those of you that are already members know the resources available through participation in InfraGard. For those of you that are not familiar with InfraGard, the following article (which can be viewed in its original form at www.fbi.gov) discusses some distinct advantages InfraGard membership brings.

INFRAGARD

A Partnership That Works

03/08/10

InfraGard today has 85 chapters with more than 35,000 members nationwide helping to protect and defend critical infrastructure.

One member gave us information about a financial institution victimized by an online banking fraud in which large sums of money were moved in and out of the company's accounts. Another let us know about an intrusion into a computer system that resulted in the defacement of a number of state agency websites. A third convinced a U.S. business to contact us when it was hit with an "SQL injection" attack that inserted code into its website, enabling crooks to gain access to a company database with customer orders and credit card numbers.

In each of these cases—and many more like them—a member of an FBI-sponsored initiative called InfraGard made a difference by sharing valuable information that benefited our investigations, the organizations involved, and the larger community.

That's precisely the point of the program, which brings together representatives from the private and public sectors to help protect our nation's critical infrastructure and key resources from attacks by terrorists, criminals, and others who wish us

harm.

It's a partnership that makes sense, since most U.S. infrastructure components—like utility companies, transportation systems, telecommunication networks, water and food suppliers, public health, and financial services—are privately owned and operated.

Early Focus on Cyber Crime

InfraGard began in our Cleveland office in 1996 as a way to share information with local information technology (IT) experts and academia in support of our cyber investigations. We passed along what we knew about cyber intrusions and crime trends to our partners to help them secure their facilities and computer networks. And our partners shared with us their IT expertise and information they had on possible cyber crimes.

The program proved so successful that we replicated it in each of our 56 field offices...and expanded its initial focus on cyber crime to include terrorism, intelligence, criminal, and security matters.

Today's Broader Focus

Now, 85 InfraGard chapters with a total of more than 35,000 members work with us through our field offices to ward off attacks against critical infrastructure that can come in the form of computer intrusions, physical security breaches, or other methods. These members represent state, local, and tribal law enforcement, academia, other government agencies, communities, and private industry.

At the chapter level, members meet to discuss threats and other matters that impact their companies. The meetings—led by a local governing board and an FBI agent who serves as InfraGard coordinator—give everyone an opportunity to share experiences and best practices.

InfraGard members have access to an FBI secure communications network featuring an encrypted website, web mail, listservs, and message boards. The website plays an integral part in our information-sharing efforts: we use it to disseminate threat alerts and advisories. We also use it to send out intelligence products from the Bureau and other agencies—last year, we posted more than 1,000 of them, and we recently gave InfraGard members the ability to offer feedback.

Dr. Kathleen Kiernan, chairman of the InfraGard national board of directors, said, "The information and intelligence flows seamlessly between everyone involved, a great testament to selfless public service."

And in terms of our investigative efforts, over the past few years we have opened hundreds of cases as a result of information provided by InfraGard members and have received assistance on more than 1,000 others.

If you're interested in joining this cause, go to InfraGard's public website at www.infragard.net or contact your local FBI field office.

For those of you that are already members of InfraGard, you might want to consider seeking membership for individuals within your organizations that are not already on board. For example, your Security staff may have membership, but are key members of your Information Technology Department members? The ever increasing universe of cyber threats are enumerated on a daily basis in the Homeland Security Daily Open Source Infrastructure Report, available to InfraGard members. Through membership in InfraGard , IT professionals can securely communicate with peers, and discuss potential or emerging threats, and learn how to prevent or mitigate them. Physical Security specialists would benefit by seeing the reports of various safety and physical protection issues arising across the country on a daily basis. Depending on your organizational alignments, some individuals working within your Human Resources Departments might benefit (primarily where information security, physical security, plant safety, and similar functions are managed or fall under the HR Department). Again, if you are interested, please visit the InfraGard web site at www.infragard.net .



The next resource to be discussed examines the best practices that can be put in place for the use of closed circuit television systems and security cameras. It is in the form of a video produced by the FBI's Operational Technology Division, as discussed below:

CAUGHT ON CAMERA

Best Practices for CCTV Systems

03/23/10

The Operational Technology Division's **Caught on Camera** can be seen here: www.fbi.gov/multimedia/cctv031610/cctv031710.htm or on our YouTube page: www.fbi.gov/cgi-bin/outside.cgi?http://www.youtube.com/watch?v=u5Oj2FDwLXs .

The TV news anchor soberly announced the day's top story: another city transit bus had been bombed, and a domestic terror group was claiming responsibility. The report went on to say that witnesses saw a man get off the bus just before it blew up, and that the FBI was investigating.

The scene described above—realistic as it may sound—is part of a fictional new video. But **Caught on Camera** is not a product of Hollywood. While it does have high production values, special effects, and narration by Annie Wersching, co-star of the TV show **24**, the video was created by our Operational Technology Division to show business owners how their security cameras can aid law enforcement investigations and maybe even help solve a terrorist attack.

Using the transit bus bombing as its story line, the 20-minute instructional video shows how closed circuit television (CCTV) systems can be installed and maintained for maximum effect—not only for the business owner but for the needs of law enforcement as well.

“Convenience stores, banks, mom and pop operations, gas stations—potentially tens of thousands of businesses could enhance their security systems with the simple tips provided by this video,” said Katrina Gossman, unit chief for the Forensic Audio, Video, and Image Analysis Unit. Buying expensive new equipment isn't necessary, Gossman added. In most cases, a few changes to existing systems can make a significant difference.

“Often the surveillance images we receive from these types of security cameras are of poor quality, and they don't need to be,” she said, explaining that such images can be critical in iden-

tifying and apprehending a terrorist or fugitive.

Caught on Camera shows how to avoid common problems such as installing cameras in the wrong places, ignoring lighting and line-of-sight issues, and having administrators who don't understand how the systems operate. "Many business owners think their systems are fine until something happens," Gossman said.

The video uses real actors as well as FBI personnel, including members of our Hostage Rescue Team. "We wanted to make a training video that wasn't boring," said Melody Buba, a forensic video examiner who worked on the year-long project. "It needed to be entertaining enough for business owners to watch it, but instructional."

In the video, the terrorist shops for bomb-making material in a local home improvement store and buys backpacks at a pharmacy to transport the explosives. Many of the stores' surveillance images are flawed, but one home improvement store camera reveals that the bomber has a distinguishing tattoo on his neck, which proves crucial to the investigation.

There are many ways for CCTV systems to fail, one of the actors explained. "But when the system works, it can make all the difference." If you are going to install a CCTV system, the video points out, "Do it right—for yourself, for law enforcement, and for your community."

In the case of Caught on Camera, the system did indeed work. And the outcome is fun to watch.

Caught on Camera is also available free of charge in DVD format to members of the law enforcement community, business owners, CCTV vendors, suppliers, contractors, and educators. To request a copy, send an e-mail to cctvdvd@leo.gov. Please include your name, position, agency, street address (no post office boxes), and telephone number.



The next resource is the FBI's Internet Crime Complaint Center (IC3), and the IC3 2009 Annual Report on Internet Crime. As you'll see below, the IC3 is a centralized location where individuals can report criminal activity involving the internet. The annual report produced by the IC3 is a useful tool to identify trends, and contains information that could be forwarded to employees to raise awareness of cybercrime threats and methodology. An article about the IC3 follows:

INTERNET CRIME

Complaints on the Rise

03/17/10

Internet crime complaints rose 22.3 percent in 2009, according to the latest IC3 report.

During 2009, did you receive an e-mail that claimed to be from the FBI and asked for money or personal information?

If you did, you're not alone—e-mail scams that misused the Bureau's name represented the highest percentage (16.6) of complaint types submitted last year to the FBI's Internet Crime Complaint Center (IC3), according to its latest annual report.

All told, IC3 received 336,655 complaints during 2009, a hefty 22.3 percent increase from 2008.

In addition to the fake FBI e-mails, rounding out the top five complaint categories were:

- **Non-delivered merchandise and or non-payment, in which either a seller didn't ship a promised item or a buyer didn't pay for an item (11.9 percent);**
- **Advance fee fraud, when a victim was asked to give money upfront, often for goods or services that never materialized (9.8 percent);**
- **Identity theft, when someone either stole or tried to steal a person's identity or some kind of identity information (8.2 percent); and**
- **Overpayment fraud, when a "buyer" sent a victim who was selling something a legitimate-looking check or money order (that turned out to be counterfeit) for an amount greater than the price of an item being sold, and then asked the seller to deposit the payment, deduct the actual sale price, and return the difference (7.3 percent).**

Of the 336,655 complaints submitted to IC3 last year, just under half—146,663—were referred to local, state, or federal law enforcement agencies for further action. Most of those cases involved fraud and financial losses by the victims. The losses from the referred cases totaled \$559.7 million.

The complaints not referred to law enforcement generally had no financial losses—for example, a victim received a fraudulent unsolicited e-mail but didn't act on it—or involved victims and perpetrators who both lived outside the United States.

But complaints not directly referred to law enforcement are still valuable—they're accessible by law enforcement and are used to analyze trends, gather intelligence, and educate the public. So if you feel you've been targeted, please submit a complaint to IC3 at: www.ic3.gov/complaint/default.aspx whether you lost money or not.

Some of the more popular e-mail scams during 2009 (and scams to watch out for during 2010) included:

- **A new spin on the "hit-man" scam www.fbi.gov/page2/jan07/threat_scam011507.htm , in which individuals received an e-mail from an "assassin" who claimed he was going to kill them, but who said they would be spared if they sent money because someone in his organization knew a member of their family and pled for their lives.**
- **Spam or pop-ups offering free astrological readings, but only after birthdates and birthplaces were provided. Victims were then enticed into purchasing a full-fledged reading with the promise they would find out something favorable was about to happen. Of course, they never received the reading.**
- **Economic stimulus scams, where victims received a recorded phone message directing them to websites where they could apply for government stimulus money after first entering personal information and paying a small fee. Needless to say, no stimulus money was received.**
- **Fake pop-up ads for anti-virus software: www.ic3.gov/media/2009/091211.aspx that warned of the existence of computer viruses but actually downloaded malicious code when clicked.**

For more information on Internet crime, read the full report at: www.ic3.gov/media/annualreport/2009_IC3Report.pdf



Another excellent resource is the www.fbi.gov web site. A broad variety of programs are discussed. Many articles are located here. A security professional, trying to answer a question asked by an employee, might find a topic discussed that helps answer the question. As an example, please see the following article from the www.fbi.gov web site:

INVESTORS BEWARE

Stock Fraud Case Offers Lessons

01/29/10

If you're not familiar with “pump-and-dump” fraud schemes, it might be a good time to get educated.

That's because the FBI and its partners are now wrapping up an investigation of such a scam that was so massive it took the better part of a decade to unravel. So far, our joint investigation has uncovered more than 40 schemes, convicted 40 perpetrators, identified thousands of victims in nearly every state and several foreign countries, and discovered hundreds of millions of dollars in losses.

In Operation “Shore Shells,” so-named because it involved fake (or shell) companies and began in the coastal area of southern New Jersey, a group of co-conspirators—CEOs, stock brokers, CPAs, financial advisors, attorneys, etc.—had been engaging in pump-and-dump and other schemes for years.

How do these scams work? In this case, the ringleaders created shell companies whose penny stock (worth less than \$5 a share) was traded on the OTC Bulletin Board (not on the more widely known New York Stock Exchange or NASDAQ). They secretly issued most of the shares for themselves in fictitious names, then touted their companies' stock through false statements in press releases, electronic bulletin board postings, online newsletters, and the like.

Often using their retirement funds, unsuspecting investors purchased the highly-touted stock—or their unscrupulous financial advisors did so without their knowledge—driving or “pumping” up the price. Then, the fraudsters “dumped,” or sold, their stock for thousands or millions of dollars, causing the stock to plummet and innocent investors to lose their shirts.

In many cases, the losses were significant. And while running an undercover operation and gathering enough evidence to put the criminals behind bars, our focus has been on helping victims get some of their hard-earned money back. We spent years interviewing more than 600 mainly elderly victims, painstakingly documenting their sometimes heartbreaking losses. For example:

- **We assisted a doctor from a prestigious hospital who began suffering from severe depression after learning of the scam and became unable to work.**

- To help a husband and wife who had both developed dementia during the investigation, our agents traveled to their nursing home and spent hours with them, their family members, and their accountants to substantiate their financial losses.
- We worked with a man suffering from multiple sclerosis whose stockbroker had liquidated his pension and IRA and left him nearly penniless.
- We learned of another victim who not only invested her savings and her pension, but also took out a second mortgage to invest more. Needless to say, she lost everything.

It was worth the effort. So far, more than 100 seizures and forfeitures totaling over \$70 million in cash, artwork, jewelry, homes, cars, and other valuables have been made, and criminals have been ordered to pay more than \$130 million in restitution. We expect millions more to be forfeited and repaid to the victims.

Because of their work on behalf of the victims in this case, the investigative team—comprised of special agents from our Atlantic City Resident Agency (out of the Newark FBI office), a Criminal Investigation agent from the Internal Revenue Service, and the Newark FBI's victim/witness specialist—was awarded the FBI Director's Annual Award for Distinguished Service for Assisting Victims of Crime.

How 'Pump and Dump' Works

First, there's the glowing press release about a company, usually on its financial health or some new product or innovation.

Then, newsletters that purport to offer unbiased recommendations may suddenly tout the company as the latest "hot" stock. Messages in chat rooms and bulletin board postings may urge you to buy the stock quickly or to sell before the price goes down. Or you may even hear the company mentioned by a radio or TV analyst.

Unsuspecting investors then purchase the stock in droves, pumping up the price. But when the fraudsters behind the scheme sell their shares at the peak and stop hyping the stock, the price plummets, and innocent investors lose their money.

Fraudsters frequently use this ploy with small, thinly traded companies because it's easier to manipulate a stock when there's little or no information available about the company. To steer clear of potential scams, always investigate before you invest.

Steps You Can Take

- Don't believe the hype
- Find out where the stock trades
- Independently verify claims
- Research the opportunity
- Watch out for high-pressure pitches
- Always be skeptical

Learn more about "pump and dump" schemes at SEC.gov: www.sec.gov/rss/your_money/pump_and_dump.htm

Another example of useful information found at www.fbi.gov is this article:

Mass Marketing Fraud—Awareness & Prevention Tips

Mass Marketing Fraud—Basic Overview

Mass Marketing Frauds target individuals of all ages and walks of life. Victims are lured with false promises of significant cash prizes, goods, services, or good works, in exchange for up-front fees, taxes or donations.

Costs of Fraud

Mass Marketing Frauds victimize millions of Americans each year and generate losses in the hundreds of millions of dollars.

The Top Schemes

Foreign Lotteries & Sweepstakes

Nigerian Letter Scams

Credit & Loan Scams

Overpayment Scams

Charity Scams

Common Scams—Be on the Lookout for Fraud

Foreign Lotteries & Sweepstakes Foreign lottery fraud is currently one of the most prevalent consumer frauds. Victims are told that they have won a lottery or sweepstakes in a foreign drawing. To collect the winnings, victims are told they must first pay various taxes and fees.

Nigerian Letter Scams Victims are asked to help illegally transfer funds out of Nigeria in return for a share of the money. Perpetrators ask victims for their bank account information under the pretext that it is needed to complete the transaction. Victims may also be asked to pay money up-front to help defray the cost of taxes, legal fees, or bribes.

Credit & Loan Scams Victims with poor or non-existent credit are offered credit cards/loans—for an advance fee. “Credit repair services” may offer to help those with poor credit improve their credit ratings—for an advance fee.

Overpayment Scams The victim is advertising an item for sale. A “buyer” sends the seller a counterfeit check or money order for more than the cost of the item. The victim is asked to return the difference between the payment and the cost of the item. When the payment turns out to be counterfeit, the victim is held responsible by his or her financial institution.

Charity Scams Con artists solicit donations in the name of non-existent or fraudulent charities. Most charity scams occur during the holidays or in the aftermath of disasters, when philanthropy is most common.

Protect Yourself—How You Can Avoid Becoming a Victim

The Hallmarks of Mass Marketing Fraud

- Offers appear “too good to be true.”
- Payments for goods or services are required in advance.
- Personal information is requested over the telephone.
- Offers are unsolicited.
- Representatives use high pressure sales techniques, claiming that immediate action is required.

What You Can Do

- Don't believe everything you are told. If something sounds too good to be true, it probably is.
- Avoid being taken by high pressure sales. Take the time to research offers before deciding whether or not to participate.
- Don't do business with anyone who solicits your money in advance of awarding a prize.
- Inspect all representatives' credentials carefully.
- Get all offers in writing and keep a copy for your records.
- Don't deposit checks sent by companies that claim the check is being sent to pay fees or taxes on lottery winnings.
- Report scams when they occur

Don't ever be embarrassed. These frauds are perpetrated by sophisticated con artists. File a claim with the appropriate entities listed at the end of this article. Report the crime promptly—you'll have a better chance of getting your money back and bringing the perpetrators to justice when you file a complaint soon after the crime.

Reporting Resources

Federal Trade Commission (FTC)

www.ftc.gov

(877) FTC-HELP; (877) 382-4357

Victims are strongly encouraged to report frauds to the FTC, which maintains a comprehensive scam database called Consumer Sentinel.

PhoneBusters

Tel: (888) 495-8501; Fax: (888) 654-9426

For frauds related to Canada, victims should contact PhoneBusters, a Canadian government clearinghouse for fraud information.

Internet Crime Complaint Center (IC3)

www.ic3.gov

For internet-based scams, individuals are encouraged to report incidents directly to IC3.

American Association of Retired Persons (AARP)

www.aarp.org

For information related to fraud schemes targeting senior citizens, individuals should take advantage of the resources available on the AARP website.

Internal Revenue Service (IRS)

(877) 829-5500

www.irs.gov

To avoid charity frauds, individuals should research organizations on the IRS website.

Better Business Bureau, Wise Giving Alliance

(703) 276-0100

www.give.org

The Wise Giving Alliance provides information on charities that have been the subject of donor inquiries and also offers tips about charitable giving.

Federal Bureau of Investigation (FBI)

www.fbi.gov

Individuals are always encouraged to report Mass Marketing Frauds to their local FBI offices.

Many readers of this newsletter have responsibilities involving physical security, safety, and the prevention of work place injuries. These duties could include the prevention of violence in the work place. Located at the following link is a document compiling the results of a Workplace Violence symposium held June 10-14, 2002. At the symposium were representatives from law enforcement, private industry, government, law, labor, professional organizations, victim services, the military, academia and mental health. Over the course of the symposium, the shared expertise of the attendees was on display in panel discussions and breakout groups. The FBI's Critical Incident Response Group, National Center for the Analysis of Violent Crime, FBI Academy, Quantico VA, compiled the resulting information, discussions, best practices, etc. into the publication **Workplace Violence Issues in Response**, located at: www.fbi.gov/filelink.html?file=/publications/violence.pdf

For readers that might have a potential interest in this publication, the table of contents is listed below:

Table of Contents

Message from the Director 5

Foreword 6

Acknowledgments 8

I. Introduction 10

II. Preventing Violence: Planning and Strategic Issues 18

 Sidebar 1: Sample Workplace Violence Policy Statement 30

 Sidebar 2: Questions in a Threat Assessment 30

 Sidebar 3: Sample Threat Assessment 32

 Sidebar 4: What Doesn't Work 33

III. Law Enforcements Changing Role 35

 Sidebar 5: Case Study of Police-Employer Cooperation 39

IV. Domestic Violence and Stalking in the Workplace 40

V. Legal Issues 46

VI. The Biggest Challenge 49

VII. A Special Case: Violence Against Health Care Workers 53

VIII. Dealing with the Aftermath 57

IX. Summary of Recommendations/Suggestions for Further Research . 60

Appendix A: Agenda 67

Appendix B: Participants 70



In the September and October issues of this newsletter, we discussed overseas travel security measures designed for the business traveler and for individuals traveling overseas for reasons unrelated to business. The following is taken from a four page slick handout titled Safety and Security for US Students Traveling Abroad. Though much of the advice is similar or identical to that contained in the previous travel security guidance, there is some content that is designed specifically for the college student traveling overseas:

U.S. Department of Justice

Federal Bureau of Investigation

SAFETY AND SECURITY for US Students Traveling Abroad

Did You Know?

Groups of children and teens may swarm you and forcibly steal your personal belongings.

“Act Smart. Be Safe.”

Living and studying in another country will be an enriching and rewarding experience, especially if you are prepared and take certain precautions.

This brochure will introduce you to threats you may face and provide tips on avoiding unsafe situations. Following these precautions will reduce your risk of encountering problems.

An ounce of prevention is worth a pound of cure

Before You Go

Familiarize yourself with local laws and customs in the areas you plan to travel. You are expected to obey their laws, which may include dress standards, photography restrictions, telecommunication restrictions, curfews, etc.

Plan your wardrobe so that it does not offend the locals, nor draw unwanted attention to yourself. Americans are perceived as wealthy and are targeted for pick pocketing and other crimes. Do not wear expensive-looking jewelry and avoid wearing American team sports shirts or baseball caps that might indicate you are an American.

Do not take any unnecessary identification or credit cards in case they are stolen. Take only what is necessary. Obtain traveler's checks and do not carry a large amount of cash.

Establish points of contact for your family to contact and for your foreign hosts to contact in the event of an emergency.

Make copies of your passport, airplane ticket, driver's license, and credit cards that you take with you. Keep one copy at home; carry a second copy with you but separate from the originals. This will help speed the replacement process if they are lost or stolen.

Take any necessary medications with you in their original containers and keep them in your carry-on luggage (not checked baggage) during the flight.

Obtain specific pre-travel country risk assessments for the country/countries you plan to visit from your study abroad program manager, the State Department, and/or the FBI. There may be specific issues you should be aware of and prepare for that will ensure your safety and peace of mind. Visit the State Department's Travel Advisory website at: www.state.gov/travel , and the Center for Disease Control for Traveler's

Health issues at: www.cdc.gov .

During Your Stay

Protect your passport! Theft of American tourist passports is on the rise. It is recommended that you carry your passport in a front pants pocket or in a pouch hidden in your clothes, and that it remain with you at all times. Some hotels require you to leave it at the desk during your stay and they may use it to register you with the local police--a routine policy. Ask for a receipt and be sure to retrieve your passport before continuing your trip. If your passport is lost or stolen, report the situation immediately to the nearest US Embassy or Consulate.

Do not invite strangers into your room.

Be courteous and cooperative when processing through customs. Do not leave your bags unattended. Stay alert.

Use only authorized taxis. Passengers have been robbed or kidnapped when using “gypsy” taxis.

Avoid traveling alone, especially after dark. Be conscious of your surroundings and avoid areas you believe may put your personal safety at risk. Be wary of street vendors and innocent-looking youngsters. It has been reported that while one person has your attention, the other is picking your pocket.

Do not carry large amounts of cash. Always deal with reputable currency exchange officials or you run the risk of receiving counterfeit currency. Keep a record of your financial transactions.

Beware that theft from sleeping compartments on trains is common.

Do not leave drinks unattended – someone could slip a drug into it that causes amnesia and sleep.

Avoid long waits in lobbies and terminals, if possible. These areas may be full of pickpockets, thieves, and violent offenders. Laptop theft is especially common in airports.

In an international airport, a thief positioned himself to walk in front of a traveler who was walking with his roll bag. The thief stopped abruptly in front of the traveler causing the traveler to also stop. A second thief was following and quickly removed the traveler’s laptop from his roll bag and disappeared.

Avoid civil disturbances and obey local laws. If you come upon a demonstration or rally, be careful; in the confusion you could be arrested or detained even though you are a bystander. Be mindful that in many countries, it is prohibited to speak derogatorily of the government and its leaders. It may be illegal to take photographs of train stations, government buildings, religious symbols, and military installations.

Avoid any actions that are illegal, improper or indiscreet. Avoid offers of sexual companionship; they may lead to a room raid, photography, and blackmail. Do not attempt to keep up with your hosts in social drinking. Do not engage in black market activities. Do not sell your possessions. Do not bring in or purchase illegal drugs or pornography. Do not seek out political or religious dissidents. Do not accept packages or letters for delivery to another location.

An American in China was given a letter by a man he had never met. He tried to return the letter but the man ran away. That evening, Chinese officers visited the American, admonished him for taking the letter, and required him to sign a statement concerning the event.

If you are arrested for any reason, ask to notify the nearest US Embassy or Consulate. A consular officer cannot arrange for free legal aid or provide bail money, but they can assist you. Do not admit to wrongdoing or sign anything. Do not agree to help your detainer.

Keep a low profile and shun publicity. Do not discuss personal or family information with local news media, and as a general rule, be careful what information you share with foreigners. They may have been directed to obtain information about you for duplicitous purposes and may use what they learn to target or use against you.

Evade criminals and terrorists by being aware of your surroundings and alert to the possibility of surveillance. Do not challenge your followers, but make mental notes about them. Promptly report such incidents to appropriate security officials and/or the US Embassy or Consulate. In general, criminals will strike when their target seems most vulnerable and lax about his/her security. If you are kidnapped, remain calm and alert; comply with orders, be non-threatening, avoid arguments, and establish a program of mental and physical activity for yourself.

“Turkey drop” scam in Russia: a person drops money in front of a victim while an accomplice waits for the money to be picked up and suggests splitting it. The first person returns and accuses both of stealing the money. This usually results in the victim’s money being stolen.

Beware of new acquaintances who probe for information about you or who attempt to get you involved in what could become a compromising situation.

Do not gossip about character flaws, financial problems, emotional relationships, or other difficulties of your fellow Americans or yourself. This information is eagerly sought by those who want to exploit you or your fellow travelers.

Beware that your conversations may not be private or secure. Unlike the United States, most other countries do not have legal restrictions against technical surveillance. Most foreign security services have various means of screening incoming visitors to identify persons of potential intelligence interest. They also have well established contacts with hotels and common hosts that can assist in various forms of monitoring you.

Two American students on study abroad talked privately about the lighting in their apartment. The next day, a light that had been out for weeks was working.

Telephone, Laptop and PDA Security

If you can do without the device, Do Not Take It!

Do not leave electronic devices unattended. Do not transport them (or anything valuable) in your checked baggage. Shield passwords from view. Avoid Wi-Fi networks if you can. In some countries they are controlled by security services; in all cases they are insecure.

Sanitize your laptop, telephone, & PDA, prior to travel and ensure no sensitive contact, research, or personal data is on them. Backup all information you take and leave that at

home. If feasible, use a different phone and a new email account while traveling.

Use up-to-date protections for antivirus, spyware, security patches, and firewalls. Don't use thumb drives given to you – they may be compromised.

During the Beijing Olympics, hotels were required to install software so law enforcement could monitor the Internet activity of hotel guests.

Clear your browser after each use: delete history files, caches, cookies, and temporary internet files.

In most countries, you have no expectation of privacy in Internet cafes, hotels, airplanes, offices, or public spaces. All information you send electronically (fax, computer, telephone) can be intercepted, especially wireless communications. If information might be valuable to another government, company or group, you should assume that it will be intercepted and retained. Security services and criminals can track your movements using your mobile phone and can turn on the microphone in your device even when you think it is turned off.

Beware of "phishing." Foreign security services and criminals are adept at pretending to be someone you trust in order to obtain personal or sensitive information.

If your device is stolen, report it immediately to the local US Embassy or Consulate.

Change all your passwords including your voicemail and check devices for malware when you return.

Cyber criminals from numerous countries buy and sell stolen financial information including credit card data and login credentials (user names and passwords).

Upon Your Return

Report any unusual circumstances or noteworthy incidents to your study abroad program manager and to the FBI. Notifying the FBI will help ensure that future travel advisories take into consideration the circumstances and incidents you encountered. It is not uncommon for foreigners to contact you after your return. The FBI may be able to help you determine if these contacts pose any risk to you.

Reminder

Our country will be judged by the impression you make. As an American abroad, you serve as a spokesperson for the United States.

Additional travel security tips were provided in previous newsletter editions and can be provided again upon request.

Your local FBI office #: 402-493-8688

