

New Membership Cards

The old membership cards all expired in September. InfraGard has issued new cards and sent them to our FBI Coordinator, Tom Leene, who still has many undelivered. If yours is among them, please act quickly. You can send Tom a self-addressed envelope, phone his office to ask that they mail your card, or arrange to stop by and pick it up. Or if you live or work near a board member, ask to pick up your card from him. Go to our Web page (<http://www.vtinfragard.org/about.html>) for contacts to Tom and our board members.

Now is also a good time to look at the back of your membership card. Here is the information you need to report an unusual activity, although it is better to call Tom Leene directly or contact a board member. Here also is how to reach at the InfraGard Technical Support Center's help desk with questions about the secure IG Web site. This is handy quick reference information you can carry with you – right there on the back of your membership card. And please be sure your membership card is the current one.

2009 Holiday Season Security Awareness

Terrorist groups and other troublemakers remain intent on attacking the U.S. and the holiday season offers them many extra opportunities and greater chances of success. The holidays provide many soft targets and make detection-deterrence-disruption much more difficult. Therefore, 'tis the season to consider what each of us can do to heighten security awareness.

Holidays offer a wide array of targets for attacks on gatherings and events, buildings and sites, travelers, communications, utilities, and more. The jihadists have long vowed vengeance on America and they remain steadfastly determined. But what might be coming? Recent overseas attacks suggest some targets here: hotels, restaurants, stores, sports and entertainment venues, religious gatherings, transportation infrastructure, and even schools and hospitals. Other seasonal possibilities here include iconic structures and prominent political, economic and infrastructure targets that may be at increased risk during holiday celebrations. Because of the diversity of holiday events, determining when, where and how an attack may occur is exceedingly difficult, especially because holiday events are well known.

Consider first the terrorists' goals: to produce mass casualties, visually dramatic destruction, significant economic aftereffects, and fear within the U.S. population. Lesser attackers, such as shooters, may simply be hate crimes, but they achieve the same effects only in smaller scale. In either case, any attack is disruptive and costly. Yet with some understanding of their goals and techniques, prevention is still possible.

There are recognizable patterns (a/k/a signatures) preceding nearly all attacks and these can be observed and reported in time to prevent trouble. Troublemakers first conduct detailed reconnaissance of the site and surveillance to determine the layout, access routes, security in place, where to stash equipment and supplies, how best to attack, and then how to get away free. Most of these activities are detectable -- sometimes by security personnel, sensors and cameras -- but more often by vigilant observers. Given the hundreds of special holiday targets, the role of vigilant observers is especially vital. People can notice and report any unusual, suspicious, threatening or too-frequent event. Then law enforcement may be able to connect the dots and intervene.

The next recognizable pattern is the several dry runs the attackers must make to determine the attack route, how to bring in and cache supplies and equipment, and plan an escape. They need to time each option and each step, and often must sometimes establish hiding places -- an obvious giveaway. The initial dry runs only move people -- nothing dangerous yet. Most of the dry runs are suspicious if carefully observed, although the attackers will make every effort that everything looks as innocent as possible.

The first line of defense is to encourage all personnel and visitors to remain alert and watchful and immediately report any unusual, suspicions or threatening situations. These include vehicles improperly stopped,

unexpected deliveries or service calls, or unattended bags or packages. Consider too the possibilities of diversions and secondary or multiple attacks. To enhance vigilance, post notices that security is in place and include instructions how to report anything unusual. Distribute security awareness articles and brochures and hold frequent security briefings. Also, rehearse the procedures if there is an intruder, smoke, an explosion, a chemical release, gun fire, or a diversionary tactic such as a screaming child, loud argument, or smoke bomb.

Before and during the holidays, institute more visible security patrols varying in composition, timing, and routes. And for lasting protection, deploy more visible surveillance equipment with automatic alarms at access points and inside critical areas and review the recordings and logs frequently for anomalies. Terrorist activity is on the increase worldwide and violence may well come to the U.S soon and be with us for some time. We must be knowledgeable and prepared, remain vigilant, and report anything unusual. InfraGard members are uniquely positioned to do this.

Scams & Scams & Still More Scams

The holidays always bring a flurry of scams intended to steal information and money. Some of the holiday trickery is old but presented in a variety of disguises and some is new and still somewhat unknown. Moreover, despite the holidays, the current trend is clear that scams are increasing in number, becoming more dangerous, and more are succeeding. Forget about security by obscurity or being somewhat prepared. You and your organization are clearly at increasing risk and you'd best examine your defenses.

We all know of emails, phone calls, letters by mail or packages by courier that warn you of a compromised credit or debit card or bank account. We also know that many donation requests are phony, and the phony checks you may receive. The same is true of emails from the IRS or other government agency, or from a lottery somewhere, or about an unknown legacy supposedly due you. We all know these are scams, don't we? So keep your head and think before you click or accept anything.

Also increasingly prevalent are skimmers attached to ATMs, kiosks or gas pumps that accept credit and debit cards. The card slot looks almost normal. But if you look carefully before inserting your card, you'll see that the slot is actually an attachment, and it has been put there to skim and record whatever information is recorded on your card. There may also be something attached above and behind you where a concealed pinpoint camera can record your PIN as you key it in. These attachments come and go quickly. What may look like a service crew can install this gear in minutes and then remove all traces just before the ATM, kiosk or gas pump is actually serviced. And there are a few used machines, bought and set up just to trick you.

Therefore, any time you even think that your card or account may be compromised, telephone the provider immediately, using only the telephone number on your card or your statement. This puts you in direct contact with the right people. Never, ever, click on a link – any link – or “dial-or-say one” to be transferred. There is a clever man-in-the-middle attack for the latter that, in fact, does connect you to the proper help desk. The attacker is muted and actually listening as you give your account number and identify yourself. The trick is that the attacker immediately uses your card or account while you are still explaining to the help desk.

Just be careful and remain vigilant. Go slowly, think and verify before you do anything.

Finally

Here we are again finger pointing, this time at whom to blame for the recent shootings at Fort Hood. Here is yet another slip-up, even after we are still looking to blame someone for 9/11 and Katrina, and the many shootings that still happen year after year. Why can't someone protect us! Why didn't they see the warning signs and stop it? The Texas incident is no different. It doesn't much matter whether this man is a jihadist or a disturbed person, who may have recruited or helped him, or whether there are still unknown accomplices. Someone should have connected the dots before the fact and intervened! Yet even now, long after all these events, many of the dots are still missing.

Problem is that we the accusers deserve much of the blame. Apparently, nobody bothered to tell the right authorities and much of what the authorities did learn was carefully stove piped so it couldn't be consolidated, shared, or fully analyzed. Once again, there was no way that authorities could connect the dots and intervene. There simply weren't enough dots beforehand. Agreed that even after many years of criticism, most authorities are shorthanded, underfunded, and ill equipped for extensive analysis. However, money alone cannot produce results. The fundamental problem is the public's complacency.

We in InfraGard can play a big role here, but we are still not doing very much. Basically, our mission is to share information with those who have a need to know. Our primary functions are to provide information to the FBI and to share information with businesses and the community, so they too can better understand the threats and, in return, are better able to report trouble or unusual events. Essentially, the role of InfraGard is to provide law enforcement with a plentiful supply of dots to evaluate, so they can better foresee trouble. While more money will help them, InfraGard members can do far more to strengthen the security of America. And perhaps we too need a little more funding to do our job effectively.

We are in a unique position to observe and report unusual events and encourage our constituents to do so also. We're not set up to do intelligence work or analysis or surveillance, but we are able to provide valuable observations and reach out to others so they do this also. We can't be complacent and assume that law enforcement will somehow discover an attack before it happens.

Sure, we're all volunteers and beholden to our jobs to pay the bills. Even so, many don't want to get involved or decline responsibility or say they are too busy. But more likely, many not bothering to look, don't quite understand what they saw and let it go, or don't want any embarrassment of being mistaken. But the fact remains that InfraGard members are in a strong position to share valuable information and we should be doing this. We also receive training and information not available to the public to help us better determine what may be unusual or a threat. In fact, we are FBI-vetted and trusted observers, whereas the public may report emotionally or use profiling or even finger an enemy. Therefore, volunteers or not, if we want law enforcement to do better, we are probably in the best position to help them.

We already know that profiling doesn't work. However, there are discernable patterns of behavior that indicate when a person is being recruited, converted, trained, or actually planning an attack. In almost all cases of violence, the precursors of each phase are observable at least to some extent so that discernable patterns emerge. Law enforcement may not know where to look until trouble actually comes. But we may be able to report many little dots of information that can point to trouble. Most troublemakers go to great lengths to conceal their activities, even to the extent that some activities are in fact contra-indicators. Some observed activities may indeed be too innocent to be credible. This is where our experience and training can come in handy, when seemingly normal activities are too usual and are in fact concealing trouble.

There is ample opportunity to do better. Yet many just continue to finger point year after year, still demanding that someone project us, while most are doing very little to help protect ourselves. The starting point is an effective reporting system that InfraGard members are uniquely able to provide.

As always, comments, suggestions and contributions are welcome.

Frank Platt, IVMA VP and Editor

[This space is available for members to list their products or services, post links to interesting sites, or contribute material of public interest. Submissions may be edited for brevity and to reduce commercial content.]

Franklin N. Platt
Office Planning Services

55 Paris Road
Stark, NH 03582

Tel: (603) 449-2211
Email: Fnplatt@aol.com

Profit from Good SecuritySM

Security Preparedness & Compliance since 1967

• Risk Management • Analytics • Due Diligence • Second Opinion • Validation • Training
