

We're Forming New Committees

We are forming two new IVMA committees: A Meetings Committee and a Membership Committee. We are also looking for a few members to assist each committee. If you are interested or know someone who might be, contact the persons below. Their addresses are on our Web site, www.vtinfragard.org.

The Meetings Committee will plan and produce our general meetings and the annual meeting that includes our elections. The heads are Gary Kessler and Joshua Silman. Their first step is a survey recently announced on our general mailing list asking for program ideas, best times and locations, etc. Anyone can take the survey. It is anonymous, short (only ten questions) and you can add comments. Here is the link again: www.surveymonkey.com/s/CVQ67YC The deadline is Monday, May 24 at noon.

Tim Cornish and Mike Stridsberg head the Membership Committee. Their role is to attract new members and to assist and orient new and recent members. We would like some committee members from other parts of Vermont who can help set up informal get-togethers to introduce our chapter, explain the resources available to InfraGard members, and let our members better know each other.

Many New Skimming Devices

There are new warnings of skimming devices installed on ATMs, gas pumps, point-of-purchase terminals, and other machines that accept credit or debit cards. The skimmer is usually an external device added to record the magnetic stripe on your card before the machine reads it. In addition, a hidden camera records your PIN. From this, they create duplicate cards that are often sold on the street.

Normally, the card reading slot is flush with the machine or slightly indented. A skimmer is small external slot mounted on top of the normal slot. It usually protrudes slightly. Look for a difference in appearance or styling from the actual machine. If any doubt, go elsewhere. Yet another emerging variant is privately owned ATMs that are not connected to any network; they just take your deposits and record you card and PIN and are always out of cash (suspiciously, after you log in). There is nothing you can actually detect. However, the installation may look cheap or tacky. These machines are usually located in out-of-the-way places, are moved frequently, and not left in any one location for more than a few hours.

Also, look around you. Along with the skimming device, there is a hidden camera set up to record your PIN numbers as you enter them. The camera usually looks over your shoulder. The camera can be a small inconspicuous object or may be hidden behind a tacked-up sign or banner. The lens will be concealed or looking from behind a small hole (maybe ¼" diameter). The clue is any object with a sightline past you to the PIN-pad. A legitimate surveillance camera will never look at your PIN.

Another problem is that skimmers are increasingly placed *inside* of a gas pump and are not visible from the outside. However, inserting your card may still feel unusual – because it is being read twice. If you suspect something is amiss, grab your card and tell the police immediately.

Be very cautious and watchful every time you use a credit or debit card. Think what you are doing, look carefully where you are putting it, be sure the process goes as you expect it, and be sure it is your card returned. Hyper-vigilance is a wise investment; any trouble will at least cost you a lot of time and inconvenience.

There is a short PDF file sent out with this newsletter with photos of one example of the many skimmers that are out there.

Please Report Suspicious or Unusual Happenings

There are increasing warnings of attacks coming on American soil and attackers who are already here and plotting trouble. So far, good luck and hard work by intelligence and law enforcement officials have prevented any major incidents. And so far, the attacks that have almost happened only seem to be probing our defenses. However, the chances of our luck holding much longer are increasingly problematic.

We demand that government protect us. Yet many still deny that they have any responsibility to try to protect themselves or others. (No, vigilantes and guns are *not* an answer and they only make matters worse.) What is missing is our telling authorities when something suspicious or unusual happens – even minor, seemingly unimportant events – so the government can investigate and better protect us. If we do not bother to let them know, how can we possibly expect the government to protect anybody? Therefore, reporting every incident is important to our own safety.

InfraGard members are in a good position to facilitate effective reporting in many ways. We can train ourselves as observers better able to spot and report trouble. We can avoid profiling which is likely to be counterproductive. We can encourage others to report and explain why and how. And we can offer to report anonymously via our own pipelines when someone does not want to get involved. We often talk with others about security issues and we can ask directly whether they have reported trouble to the FBI.

If anyone sees trouble actually happening, call 911 immediately to alert the police. If something unusual or suspicious is happening, call the FBI immediately or let an InfraGard member do this for you. The FBI's phone numbers are in the front of every telephone directory. In Vermont, call the FBI at (802) 863-6316. Think ahead and sort out what happened and be ready to explain it coherently. Note it beforehand if you can. Otherwise, keep repeating salient facts so you will better remember them.

It's All About Information Sharing

The official mission of InfraGard is education and training. However, we can also accomplish this very efficiently by facilitating information sharing. We need to promote this, especially in ways that others cannot do as well, as quickly, or as inexpensively. First, we can facilitate information sharing in confidence among system owners and operators. This is best accomplished by forming sectors and by utilizing non-disclosure agreements to assure privacy and confidentiality. We can then redact and censor the information so that no individual, organization, system, or place can be identified. We can then share the non-identifiable information with the government, the private sector and the public. Finally, we can make sure that suspicious or unusual happenings are shared with the FBI. We as InfraGard are uniquely qualified to provide all of these services and often do so faster, better, and at much less cost than any other organization, vendor, or association or trade group.

Our mission is to implement the NIPP and form effective CIKR sectors. Our mandate goes back to HSPD-7 and PDD-63, the directives signed by Presidents Bush and Clinton, respectively, which resulted in the formation of InfraGard.

Some explanation: The National Infrastructure Protection Plan (NIPP) is a part of the Department of Homeland Security and was established by Homeland Security Presidential Directive Seven (HSPD-7) following 9/11 and signed into law in December 2003. The title is *Critical Infrastructure Identification, Prioritization, and Protection* and its purpose is to provide "a collaboration for National Infrastructure Protection." NIPP established the Critical Infrastructure and Key Resources (CIKR) sector groups – basically, special-interest groups – and these are the same sectors that each local InfraGard chapter is supposed to form. And before all this, InfraGard actually sprang from Presidential Decision Directive 63, *Critical*

Infrastructure Protection, signed in May of 1998 – about the time that the President and his NSA, Richard Clarke, were becoming concerned about the dangers of al Qaeda attacking America. Problem is that while PDD-63 is clear and includes implementation, HSPD-7 is neither. In effect, InfraGard is supposed to support NIPP, but what they mean is we should help to implement it.

The FBI provided \$400,000 in special funding to InfraGard this year, specifically so that local chapters could better support the NIPP. For our part, IVMA proposed a pilot project to form an Energy Sector to include all of the electrical utilities operating in Vermont. We would organize the group, set up procedures to privately and confidentially share information, have each participant join InfraGard for vetting and access to the member benefits, and run the first few meetings. This would be a pilot project, because our previous attempt failed and now we want to figure out how to do this right so that other chapters can follow. The problem is that only a few of us can work during business hours and in doing so would forego income and absorb many expenses as a result. We proposed to reimburse and compensate them to some extent. However, it turned out that this runs afoul of a funding requirement that members cannot be paid. We looked at some other possibilities, but none made much sense here in Vermont, so we passed on this funding opportunity in favor of other local chapters. However, we still think that an Energy Sector is well worth pursuing, so we are still exploring the possibilities and looking for other funding.

Finally

We are suggesting that IVMA form an Energy Sector to include all of the electrical utilities operating within Vermont. Its purpose is to better protect the Vermont Electrical Grid. We will work with state and federal authorities to determine how best to do this, and then meet with the utilities and trade groups to explain the benefits and value and how best to assure the necessary privacy. Without carefully paving the way, forming a sector will only be a social gesture and unlikely to provide any information useful to anybody. Indeed, we believe that to enhance public awareness goes in the wrong direction.

The problem is that to do this, many volunteers will need to spend 100s of hours, travel 1,000s of miles, and possibly do some overnights as well. There is no other way to organize this effectively. Many of our people cannot get away from their day jobs and those who can are self employed and will suffer loss of income. The solution is to offer at least an honorarium and travel expenses to our people. We need funding, maybe from the industry, a trade group, or another government agency. However, we can offer considerable value in return.

We believe the time to do this is now, to help strengthen the security and resiliency of the Vermont Electrical Grid and ward off trouble that will surely come.

As always, ideas, comments, and suggestions are welcome.

Frank Platt, IVMA President and Editor

Franklin N. Platt
Office Planning Services

55 Paris Road
Stark, NH 03582

Tel: (603) 449-2211
E-mail: Fnlplatt@aol.com

Profit from Good SecuritySM

Security Preparedness & Compliance since 1967

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