C E R T

COMMUNITY EMERGENCY RESPONSE TEAM

BRECKSVILLE – BROADVIEW HEIGHTS

General Meeting Minutes

Date: 1/20/2010

Time: 7pm-8:15pm

Location: Brecksville Community Center

General announcements were given by Jill Gerber followed by Logistics Coordinator Jim Steiger discussing issues related to cyber security.

A. General Announcements

1. Newsletter
   The winter newsletter was distributed which contained the yearly meeting schedule.

2. Upcoming Events
   The following upcoming events are available for those interested:
   a. Red Cross First Aid, January 30th 6:30pm-9pm, Downtown Red Cross
   b. H1N1 POD, January 31st 12pm, Cleveland Hts.
   c. FEMA Training, April 17th, 24th and May 1st , Contact Brian Russo

3. Help Needed
   The following positions are available; please contact Carolyn if interested in helping out:
   a. Welcome Wagon—A few members are needed to send welcome e-mails or phone calls to new members.
   b. Phone Call Committee—A few members are also needed to contact those members without e-mail about upcoming events.

4. T-Shirts
   Short sleeve T-shirts will be available for each active member. Long sleeve T-shirts, polo shirts or hooded sweatshirts may be available for purchase in the future.

5. Upcoming Events

   The following upcoming events may be scheduled in the future:
   - Winter Search and Rescue
   - Traffic & Communication Drill
   - FEMA Refresher course
   - CERT Scavenger Hunt

6. H1N1 Follow-up

   The Brecksville Chief of Police, Chief Egut and the County Board of Health thanked us for our participation in the H1N1 vaccination clinics. The first event in November went well but the December POD was even better. The Cuyahoga Valley Career Center site was used in December and worked much better than the Middle School site. A future option may be to use the High School for a staging area with the CVCC as the inoculation site.

7. ID Badges

   Anyone that needs their ID Badge picture taken can see Carolyn tonight after the meeting.

B. Cyber Security—Jim Steiger

1. The following handouts were made available for reference:
   a. Cyber bullying Glossary
   b. Glossary of Computer Crime Terms
   c. Chat Abbreviations
   d. Internet Safety & Responsibility

2. Some common terms to become familiar with:
   - Phishing—a ploy to trick people into giving up sensitive information
   - Trojan—a program that is installed without you knowing about it
   - Zombie—your computer becomes controlled by someone else
   - Virus—corruption of data or programs by an outside force
   - Spyware—programs that spy on your internet usage and report back to a company or organization
   - Spam—junk e-mail, 210 billion e-mails are sent each year, 70% of them are spam
   - Browser—allows you to view web sites
   - URL—Uniform Resource Locator, a web sites address, the domain name is the .com, .net, .us extension.

- IP address—the way computers connect to the internet and talk to each other

3. Recognizing dangers on the internet and using security in layers:
    - Reduce spam by deleting all other email address from a message before forwarding it
    - Recognize false email address trick, when something is added before or after a trusted email address i.e. brecksville.oh.us/
    - Recognize phishing attack by hovering over address before clicking on a link to see if address matches. Most phishing attacks do not use your name, they require an immediate or urgent response and the grammar is very poor. They typically ask for sensitive information such as name, address, credit card number and account passwords.
    - Perform “who is searches” to gather more information about suspicious contacts
    - Safe surfing, always understand what you are doing, be aware of which web sites may be dangerous
    - Keep security up to date and know your software
    - Use strong passwords which contain both letters and numbers
    - Don’t post or share sensitive information
    - Understand what information is sensitive, two pieces of non-sensitive information can combine to make one piece of sensitive information
    - Trust the website, look for the “https” prefix and the lock symbol which means secure
    - Use as few credit cards on-line as possible and with low limits. PayPal works well and takes care of the transaction for you
    - Don’t keep a file of passwords on your computer or a hard copy in your desk, memorize your passwords
    - Banks will send routine mail to verify any information; they will not send e-mails for this purpose.
    - Don’t click on a link, go to the website if you are suspicious
    - Snail mail attacks may happen which direct you to use your computer
    - If you do keep sensitive information on your computer use a non-typical format such as: XX XX XX XX X (social security number) instead of XXX XX XXXX, or store it on a flash drive instead of your hard drive.
    - Backup everything onto multiple computers, formats or use external hard drives. Keep copies of original software; most software can be installed up to 5 times. If you need more, call the company to give you more copies.

- Firewall security does not allow intrusions, don’t have more than one firewall product installed at a time.
- Keep virus programs updated, multiple scanning malware software is ok to have
- Turn off your computer at the end of the day, your automatic updates will occur when you turn it back on

4. Protecting kids
    - Security and electronic services may be used to limit your childs use of the computer however many 10-12 year olds can figure out how to get around it
    - Monitor children’s use of the computer frequently. Educate them on the risks of the internet
    - Give them specific guidelines about what they can and cannot do
    - Make sure they know to ask you before downloading or buying anything
    - Don’t let them create multiple e-mail accounts
    - Insist that they provide you with usernames and passwords

Respectfully Submitted,

Sue Schindler

Cc: E.Egut, J. Hajek, C. Jatsek, P. Koss