QCS Meeting Review
Scams, Frauds, and Identity Theft
Presented by Cpl. Hank Jacobsen, Davenport Police Department
Review by Joe Durham, Co-Editor, QBits, Quad-Cities Computer Society, IA
joseph85_us (at) yahoo.com

Cpl. Hank Jacobsen visited our club to share insight and advise from a policeman's perspective on the evolving scourge of the 21st Century: scams, fraud, and identity theft.

First, he described how these technological threats affect everyone when not prevented. Most victims realize something is not right and fall for the theft anyway. Young people don't realize that the theft of their Social Security Number will affect them in manifold ways in the future: car loans, credit applications, employment complications. Older citizens can lose money that they cannot afford to miss. He said that once your money has been lost it is very difficult to recover, it is usually lost for good. So, it is incumbent upon everyone to learn about these current financial and personal threats.

What is the scope of the criminal's approach to technological crime? Hank observed that criminals do this work, because it is easy for them. They are fishing for that one victim out of thousands that will succumb to their wiles. They target places and people that have a great deal of money: individual, companies and banks. So, by following his simple, commonsense solutions you can protect yourself from this mayhem.

He stated that we often say to ourselves and others:

"Everything has been fine thus far, nothing has happened to me."

It only takes that one time and you will be sorry for it right then.

The thief is always seeking that one piece of information that they need to complete their work. Our names, addresses and phone numbers are usually public. These pieces are not what they need to advance their crime. They need your social security number to give that automatic access to your account, create new accounts and transfer funds to them.

Social Security Number
Hank stated that we should keep our Social Security Number private and protected. This means that we do not carry our Social Security card with us in our wallet or purse. Some members of the audience mentioned that their Medicare card has the SSN# on it. He said that, by next year, Medicare cards will not have that full information on it. In the interim, he suggested you make a photocopy of your Medicare card and use a permanent marker to black out all but the last four digits of your number.

To follow this trend of protecting your identity, he said you should remove or shred documents that have any personal information on it. Thieves will go through dumpsters looking for information like this. Shredding this information is best. It is always a good idea to keep a separate inventory of your wallet and your purse so you can figure out what may have been pilfered by a thief.

Personal Checks
Another financial vulnerability is checks. Whenever possible, don't use checks for payment when you are out and about. Checks provide thieves with just the information they need. And, if you do use a check, just take one with you not the whole checkbook and make a notation of its use when you get home.

If possible, mail your checks by taking them to the Post Office or a USPS mailbox yourself. There is a chance a thief will look in your personal mailbox and help themselves while it is sitting there waiting to be picked up by the letter carrier.

Hank noted that banks and financial institutions mail out statements with your information on it. HIs hope is that, in the future, they correct this oversight. For the near term, make a note of when your statements arrive in the mail each month, and notify the bank if they do not arrive on the usual date.

Credit Cards
Whenever possible, use credit cards for your daily transactions. And travel with no more than two credit cards in case your wallet or purse are pilfered or stolen. It is easy for you to then contact your provider and notify them it was stolen and you can obtain a new card.

Hank does not like Debit cards. These cards have access directly to your money. If these are compromised or stolen you will immediately surrender your funds. With credit cards, you have the opportunity to notify the credit card company and your liability is limited to $50.

Credit card skimmers are the latest financial threat to our money. Thieves will surreptitiously install a card reading device on an ATM machine or a gas pump. They will also install a small pinhole camera that is very hard to see with them; so that the skimmer will read your credit card strip information while the camera records the password you enter on the numeric keypad. Once that information is matched, the thief can do anything with it.

To protect yourself against this fraud, Hank suggested that you examine the credit card slot closely to see if it is physically secure. Often times you can physically pull out these skimmer devices. On gas pumps, some thieves have placed these skimmers inside the machine to avoid detection. He suggested that you examine the state seals on the pump to make sure that they are not broken or tampered with. If they are compromised notify the authorities immediately and do not use that pump.

Unfortunately, there are hand-held skimmers that are on the market. These devices will allow someone to get close to you and in a wireless fashion obtain the strip information from your card. You protect yourself form this approach by placing your cards in a metal case or placing them inside aluminum foil.

Hank said that there are occasions when large companies have had the security of their credit card databases broken. In this event you, request a new card immediately, and closely monitor your credit card statement for any irregularities and report them.

Phishing
This is an email with content that looks like an official company website that also, conveniently asks for your site password or personal information. He said never to do anything with these emails, put them in your spam folder or trash folder.

Emails
Hank described how we should handle emails in general. Do not open link attachments in your email even if they are from a known contact. When you open up these attachments, you have given permission for their malicious code to enter your computer. Make sure to contact your sender directly to confirm that they have just sent you this particular email and attachment before opening up an attachment from a friend.

Passwords
He noted that it is difficult to keep multiple passwords and remember them. This is always a continuing challenge for the average user. Create a couple of good long passwords, write them down and keep them in a safe place and use those.

Hank closed with 4 simple rules:
1) Do not answer the phone to anyone who is calling on behalf of institution that you use. They will never start a request over the phone.
2) Don't answer the phone. Let people leave a message. If they really want to get in contact with you they will leave a message.
3) Do not make any hasty decisions or permit anyone to intimidate you into doing so. Take your time and check all areas of the request if it needs to be made.
4) You have the right to obtain a copy of your credit report once a year from the three top credit rating agencies and he recommended that you do so. One of the unfortunate drawbacks is that you have submit your SSN# to identify yourself when making the request.