SCAMS

Parking Lot Scam

It's called "a friend in need" scam and it takes a variety of forms. The parking lot one is one of them but so is...

- need to use your phone
- I'm a long lost relative
- We were in the neighborhood
- I'm collecting for a charity
- Be responsible in your giving.

On a Friday shopping trip to Costco, I was approached in the parking lot as I was about to put my groceries in the car. A woman in her thirties approached me and said that she and her children had just left an abusive relationship and wasn't able to get a cheque from Welfare until Monday. She was very embarrassed to ask, but could she please borrow $10 until Monday in order to buy milk and bread for the weekend.

Being suspicious of scams, I responded that I had no cash and had purchased my groceries with my debit card. I then offered to give her some bread from my shopping cart. She declined and said she'd ask someone else.

Her response to my offer further aroused my suspicion, so I went back into the store and spoke to their security people. They were not surprised and went out to speak to this individual. Upon their return, I learned that this particular individual has been hanging around their parking lot, approaching shoppers on a regular basis for 2-3 years. She sometimes brings her daughter along with her, and always has a different hard luck story.

Most people don't question her situation and immediately respond with usually $20. If this individual gets $20 from just 5 people a day, she's taking in some $2000 - $3000/month - a pretty good living for begging!

People are afraid not to respond "in case her story is true." If it were true, there is "Emergency Social Services" available for evening and weekend situations, and this person could always ask the police for help.

Remember that people like this continue to exist because good hearted citizens continue to respond by opening their wallets.

Please remember folks, this is just another form of fraud.

VISA & MASTERCARD
Telephone Credit Card Scams

Those con artists get more creative every day. The scam works like this:

Person calling says, "this is, and I'm calling from the Security and Fraud Department at VISA. My Badge number is 12460. Your card has been flagged for an unusual purchase pattern, and I'm calling to verify. This would be on your VISA card which was issued by bank. Did you purchase an Anti-Telemarketing Device for $497.99 from a marketing company based in Arizona?" When you say "No", the caller continues with, "Then we will be issuing a credit to your account. This is a company we have been watching and the charges range from $297 to $497, just under the $500 purchase pattern that flags most cards. Before your next statement, the credit will be sent to (gives you your address), is that correct?"

You say "yes". The caller continues... "I will be starting a Fraud investigation. If you have any questions, you should call the 1-800 number listed on the back of your card (1-800-VISA) and ask for Security. You will need to refer to this Control #" The caller then gives you a 6 digit number. "Do you need me to read it again?"

Here's the IMPORTANT part on how the scam works.

The caller then says, "he needs to verify you are in possession of your card". He'll ask you to "turn your card over and look for some numbers. There are 7 numbers; the first 4 are your card number, the next 3 are the 'Security Numbers' that verify you are in possession of the card.

These are the numbers you use to make Internet purchases to prove you have the card. Read me the 3 numbers". After you tell the caller the 3 numbers, he'll say,"That is correct. I just needed to verify that the card has not been lost or stolen, and that you still have your card. Do you have any other questions?"

After you say No, the caller then Thanks you and states, "Don't hesitate to call back if you do", and hangs up.

You actually say very little, and they never ask for or tell you the card number.

What the scammers want is the 3-digit PIN number on the back of the card. Don't give it to them.

Instead, tell them you'll call VISA or Master

card direct. The real VISA told us that they will never ask for anything on the card as they already know the information since they issued the card!

PINHOLES AND P.I.N.S.

Isn't technology grand! You combine video technology into tiny pinhole cameras, the Internet, and prices that have been driven down by demand and suddenly there are no secrets.

Some of these cameras can easily be concealed in some very standard household and common business items. VCR cassettes, motion detectors, clocks, smoke detectors, books, pictures and cell phones have all been converted into video cameras.

With cameras as small as one inch by one inch easily available and easily affordable this technology is being used in a manner that can compromise your bank and credit cards.

These cameras are being combined with current technology that reads the information stored on the magnetic strip in these cards and the P.I.N.S. are being read by covert video cameras.

New cards are being created by the criminal and bank accounts are emptied and credit cards are maxed out.

HEADS UP !

- Conceal your PIN when you use it.
- Obscure the keypad with your other hand.
- If you need reading glasses, put them on, the further you stretch out your hands the more your PIN will be compromised.
- Be aware of your surroundings. Do not use ATM machines that allow people to loiter about. Shoulder surfing is often used to obtain PIN numbers.
- Use a different PIN number for each card. Most people use the same PIN number for everything and some situations create a better opportunity for compromising that number (gas station keypads located on the pumps).

NIGERIAN LETTER SCAM

In a joint Press Release from The Edmonton Police Service, The Royal Canadian Mounted Police K Division, The Better Business Bureau of Northern and Central Alberta and the Heads Up Fraud Prevention Association, Albertans are being warned about an increase in the Advance Fee Fraud known as the Nigerian Letter Scam.

Originally as a postal letter, then as a fax and now as email this fraud begins as a request from the sender for "help" in retrieving money from foreign countries and accounts, in exchange for a substantial return.

Most of the perpetrators pose as bank auditors, a senior official or relatives of a deceased or disposed heads of states from Nigerian or other African countries.

The potential victims are often asked to turn over personal banking details, passport information, and are asked to provide a sum of money to help expedite the financial transaction.

Once the money is turned over the perpetrators disappear, often outside the authority of local officials and laws - the likelihood of arrest and recovery of funds is very slim.

The new twist on the scam is to send a bogus cheque to 'victims', with instructions to pay their outstanding debts and wire the remainder back. By the time the check is returned the funds are long gone, leaving the 'victim' on the hook for thousands.

Do not reply to these requests.

The simplest solution is to simply delete the message.

If it sounds too good to be true, it probably is!