BUSINESS WARNING: 3 SCAMMER ALERTS TIPS & TRICKS

CREDIT CARD MACHINE – POINT OF SALE MACHINE - MANUAL OVERRIDE SCAMMER PUNCHES IN STOLEN CREDIT CARD NUMBER

Point of sale machine also called Countertop Terminal and Wireless Terminal

HOW THE SCAM WORKS

1. The Point of Sale machine is handed to the customer. The employee walks away to give the customer privacy while they input their PIN number.
2. The scammer does not put the credit/debit card all the way into the machine.
3. The scammer is very familiar with how the point of sale machine works and proceeds to go through the Manual Override procedure and proceeds to manually punch in stolen credit card information into the machine. (There is a MANUAL CARD ENTRY procedure.)
4. The sale is accepted and the scammer walks away with the merchandise.
5. You later find out that a stolen credit card was used and the banks are asking why you used the manual override code. Your business is stuck with the unpaid bill.

POLICE ADVICE:

Make sure the card is pushed all the way into the point of sale machine and watch that the customer only punches in a 4 digit PIN code and nothing else.

Do not walk away from the point of sale machine thinking you are giving the customer privacy. There is a small shield on the machine that already provides privacy.

If the customer starts punching in more than the standard 4 number security PIN – CANCEL THE TRANSACTION and have them do it the proper way

If the customer complains that you are standing there watching them punch in their PIN number, tell them you have been warned by local police that scammers are manually punching in stolen credit card numbers.

The point of sale machine comes with a standard default Manager Password that should be changed to become your individual store password.

The factory default Manager's Password on your point of sale machine is similar to the password you receive when you buy a garage door opener.

When you buy a new garage door opener it comes with a standard default password. Once you install the garage door opener you need to change the password so that only your family knows the code. Most people do not change their garage door opener password and keep the factory default password. Thieves can drive down a street pressing a portable garage door opener (for a certain brand) and all the garages that have not changed the default password will open up if they have that brand of door opener installed.

So scammers that know how to use a point of sale machine may punch in the factory default Manager's Password to gain access to your machine at your business because you have not changed the factory password.

NOTE: Fraudulent cards are often damaged on purpose so the magnetic strip cannot be swiped. Instead, the customer may insist the clerk manually key in the card number, which bypasses the antifraud features of the magnetic strip.

CANADA REVENUE AGENCY (CRA) TELEPHONE SCAM – PAY YOUR TAXES BY BITCOIN OR BE ARRESTED

The entire goal of this scam is to trick you into sending them money by Bitcoin.

This phone scam has been active across North America for years and is probably originating from illegal call centres in India.

DO NOT TRUST YOUR CALL DISPLAY BECAUSE NUMBERS ON IT CAN BE SPOOFED (FAKED)

IF YOU STAY ON THE PHONE YOU MAY RECEIVE CALLS FROM THREE DIFFERENT SCAMMERS OPERATING OUT OF THE SAME OFFICE

Scammer #1 The first scammer pretends to be a CRA employee calling to say you owe money. The call display will show "Canada Revenue Agency"

Scammer #2 The second scammer pretends to be a local police officer calling to confirm there is an arrest warrant. The call display will show “RCMP”, “Vancouver Police”, “604-717-3321 (tel:(604)%20717-3321) ”

Scammer #3 The third scammer pretends to be a Crown Prosecutor or local Accountant calling to say you need to pay immediately.

You could receive a phone call from the phone scammer three different ways:

1. Individuals receive a voice message on their phone or home answering machine to call the Canada Revenue Agency back at a specific 1-800 or a 1-877 telephone number, OR

2. Individuals see a 1-800 or a 1-877 number recently called to them so they call the same number back, OR

3. Individuals answer the phone and a Telephone Scammer who claims to work for the Canada Revenue Agency is calling.

HOW THE SCAM WORKS

The CALL DISPLAY on your phone will show the “Canada Revenue Agency” or their 1-800 telephone number – it is fake.

The telephone scammer might know your name and where you work making you think that it is a legitimate call but it is not. Scammers can obtain some of your personal information from phone lists or just perform their own Internet open search of your information such as from LINKED IN.

The scammer will tell you that you owe tax money to the federal government and that if you don’t pay today the local police will come and arrest you.

The first telephone scammer will tell you that a local police officer is going to phone you to confirm the arrest warrant. This is another fake caller. The CALL DISPLAY may read “RCMP” or “Vancouver Police” or “717-3321”. The scammer will tell you that if you don’t pay your taxes right away you will be arrested.

Another scammer may call you and claim they are an ACCOUNTANT or they are a CROWN PROSECUTOR. These are fake also.

People have been kept on the phone from 2-3 hours while the scammer sends them all over the city to pay at bitcoin machines. There is a $5000 limit on Bitcoin deposits. The scammer instructs the victims to not talk to anyone otherwise the fine can increase.

(NOTE: In the recent past the scammers were getting people to buy gift cards but now they want people to use Bitcoin machines.)

Some Bitcoin machines actually have signs posted telling people not to use the machine to send money to the CRA because it is a scam. But people ignore the signs.

POLICE ADVICE: No government agency or any police department in Canada is going to telephone you and threaten you with arrest if you don't pay in Bitcoin or gift cards. Just hang up the phone and ignore the calls.

BC HYDRO TELEPHONE SCAM – PAY BY BITCOIN / GIFT CARDS - OR THE POWER IS DISCONNECTED IMMEDIATELY

1. A Telephone Scammer claiming to work for BC HYDRO could call your business telling you that you have an outstanding bill and need to pay right away otherwise the power will be disconnected. (They usually call late in the day when the restaurants are busy) They will be aggressive.

2. The CALL DISPLAY shows a BC Hydro number so you think it's real but it is fake. The telephone number on your call display has been spoofed.

3. The scammer will ask for your business email and then will send a fake invoice with a BITCOIN account number. (The email may have spelling errors and does not have the BC Hydro logos and header information). The scammer will not want you to pay through your bank account. They will insist on BITCOIN.

NOTE: the old scam was to get you to go buy gift cards and tell them the activation codes over the phone.

4. The scammer's email address may be custormersupport@bchydro.com (mailto:custormersupport@bchydro.com) (Notice there is an added "R" hidden in the word customer so the scammer can make the email look like the real BC Hydro email.)

5. The Subject line in the email may read "Eletric Payment" where the word electric is spelled wrong.

6. The scammer will pressure the business owner/employee to go immediately to the nearest BITCOIN machine and pay the fine. They will make up an excuse why you shouldn't pay at the bank. They will be very aggressive.

POLICE ADVICE: Tell the caller that you have been warned by police about the telephone scam and that you will only pay your bills the regular way. Tell them BC HYDRO does not ask its customers to pay by BITCOIN or GIFT CARDS. Then hang up the phone.

The real phone number for BC Hydro is 1 800 BCHYDRO (1 800 224 9376 (tel:(800)%20224-9376))

ADVICE FROM BC HYDRO (taken from their website)

Scammers continue to find new ways to try to trick customers into sending along personal information or, in other cases, to get them to pay money for supposed overdue BC Hydro bill amounts.

How the Bitcoin scam works

The latest scam invokes the use of Bitcoin. It's similar to an earlier (and ongoing) telephone scam in which fraudsters posing as BC Hydro employees contact customers by telephone and ask them to

purchase a cash gift card to pay for their overdue account and avoid disconnection of their service. This time around scammers tell customers to pay with Bitcoin.

The "Bitcoin scammers" email customers a bar code (or QR Code) with the scammer's Bitcoin wallet information, with the email coming from the fictitious customersupport@bchydro.com (mailto:customersupport@bchydro.com) . This message is a scam. Thinking that they're paying their BC Hydro bill, the customer takes the barcode to a Bitcoin ATM - details of locations nearby provided by the scammer - where it is scanned to complete a deposit of cash to the fraudster.

See below details on a longstanding phone scam that asks for payments via gift card.

A reminder: We don't collect credit card or bank account information over the telephone and we don't accept payment by cash gift cards or Bitcoin. If you receive a suspicious phone call from someone claiming to represent BC Hydro, hang up and call 1 800 BC HYDRO (1 800 224 9376 (tel:(800)%20224-9376)) to verify the call. Phone spoofing technology can make incoming calls appear as though they're legitimately coming from us, so it's always better to hang up and call us back to confirm.

How the email phishing scam works

An email phishing scam that has been around for months and typically comes via text message and has the appearance of an Interac e-transfer.

BC Hydro customers are being contacted by text message and email with what appears to be a notification from Interac with a link to receive a refund from BC Hydro.

Customers are told to click on a link to access their account refund by submitting their banking information.

This message is a scam: it's not from BC Hydro, and it's an attempt to obtain your private banking information.

We don't issue e-transfers or send account info via text

Please take the time to spread the word to family and friends that this is a scam.

We don't currently issue refunds via Interac e-transfer and we won't communicate with you about your account through a text message.

If you've signed up for MyHydro, you can see the latest information for your account, including your account balance, by logging in to your account at bchydro.com (http://bchydro.com/) . You can also give us a call with any questions.

If you receive a fraudulent text or email

If you're ever unsure about whether a communication from BC Hydro is legitimate, don't click any links or open any files sent to you. Call our customer team at 1 800 BCHYDRO (1 800 224 9376 (tel:(800)%20224-9376)) for clarification.

Earlier phone scam focused on gift cards continues

Reports also continue of a phone scam BC Hydro initially warned customers of in 2014. Fraudsters posing as BC Hydro employees contact customers by telephone and ask them to purchase a cash gift card to pay for their overdue account and avoid disconnection of their service.

We don't collect credit card or bank account information over the telephone and we don't accept payment by cash gift cards or Bitcoin. If you receive a suspicious phone call from someone claiming to represent BC Hydro, hang up and call 1 800 BC HYDRO to verify the call.