Gift Card SCAMS you can SPOT and EASILY AVOID!
By: Shelley Hunter

WARNING: NO government agency or reputable business will EVER ask for payment with gift cards. **NOTE: This article references US but is as applicable to Canadians.**

If someone offers to pay you money to buy gift cards… STOP!

What is a Gift Card Scam?
Gift card scams don't happen that often, but there are a few you can spot and easily avoid! Compared to credit card fraud and other forms of identity theft, gift card theft is actually quite small and the damage done is generally limited to the value of a gift card. But it doesn't matter if fraud is prevalent or not when you are the one with a gift card that does not work.
So let's look at the various gift card fraud schemes that can happen and identify warning signs that something could be amiss. Though scammers can be tricky and pretty persuasive, you generally should be able to avoid gift card scams by following the tips below.
The top gift card scams are listed (somewhat) in the order of popularity. The IRS Gift Card Scam, for example, is in the news right now as is the Balance Check 3-Way Call. So I will cover those first and then go down the list of fraud schemes to watch for.

1. Must Pay with Gift Cards (IRS and iTunes)
HOW THE SCAM WORKS: A customer receives a threatening voice message from a scammer pretending to be from the U.S. Internal Revenue Service. To avoid being arrested for tax evasion, the victim is told that he or she can pay the fine with iTunes gift cards or other gift cards. In a similar example, a "State Trooper" calls to say that the victim failed to show up for jury duty and there is warrant out for his or her arrest. To avoid going to jail, "bail" can be be paid using "MoneyPak" as a bond until the case is cleared.

Once gift cards are purchased, the scammer will ask the victim to repeat the gift card numbers over the phone–at which time, the scammer drains the value of the gift cards. Victims who fall for the initial ploy are often told to go back to the store to buy additional gift cards.

Quick Tips!
1. Hang Up on Fake Callers. No reputable company nor government agency (including the IRS / Revenue Canada) will ever demand payment with gift cards. If someone claims to be from them**.** **hang up**. (Don't believe emails either.)

2. Balance Check in Private. If someone asks to listen as you call to confirm the balance of a gift card, it is likely a scam.

3. Inspect Gift Card Packaging. If the packaging looks tampered with or the PIN is revealed, turn the gift card into the cashier and pick a different card.

4. Check the Activation Receipt. Be sure the gift card number listed on the activation receipt matches the gift card you receive. Alert the manager if it's not a match.
5. Only Buy from Reputable Resellers. Only buy discount gift cards from a gift card reseller that has customer service and will give you a money-back guarantee on purchases.
6. Save Activation Receipt. Whenever you buy a gift card, save the purchase and activation receipt until the gift card is redeemed.
On the surface, this scam seems really easy to spot and hard to believe, but given that Americans have been swindled out of nearly $40 million from it, there is obviously more to the story. According to this article on the IRS iTunes gift cards scam, "scammers posed as U.S. Internal Revenue Service officials and left victims voicemails accusing them of tax evasion and threatening them with arrest." The article goes on to say that the callers were highly trained and very convincing.
RED FLAG: No reputable company nor the IRS / Revenue Canada or any government agency will ever demand payment via gift cards.
WHAT TO DO: If you get a phone call from someone telling you to make a payment with gift cards, hang up the phone. If you get an email from a company telling you to make a payment with gift cards, delete it. Don't be fooled. If you have any doubts that the call or email is legitimate, contact the company yourself. Don't call the number given to you on the voice message, and don't respond to the email or click any of the links inside of it. Initiate the call yourself.

2. Balance Check 3-Way Call
HOW THE SCAM WORKS: A person lists a gift card for sale on a classified ads website. When an offer is made, the buyer asks the seller to confirm the balance on the card by calling the merchant in a three-way call. While listening to the seller enter the gift card number, the buyer records the touch tone numbers entered to intercept the gift card number. The fake buyer then uses the gift card number without paying for it.
Although this scam seems pretty obvious in hindsight, people are often fooled because the scam simply makes sense. It's natural that a person buying a gift card would want proof of the gift card's balance before completing the transaction. In this article on how gift cards are drained, a victim from Ohio explains how he lost a $400 Best Buy gift card because he allowed the buyer to listen in on a three-way call as he confirmed the gift card balance. Shortly after he hung up the phone, someone used the Best Buy gift card to make a purchase in California. Lesson learned.
RED FLAG: If someone asks to listen to your balance inquiry phone call or wants to look over your shoulder while you enter the numbers, it's probably a scam.
WHAT TO DO: The best way to avoid this gift card scam is to only sell gift cards to a reputable gift card reseller that offers a money-back guarantee or to take the gift card you don't want to a gift card exchange kiosk.
3. BOT Steals the Gift Card Balance
HOW THE SCAM WORKS: Hackers use a bot called GiftGhostBot to run through a store's online gift card balance check system looking for a match–meaning a valid gift card number with an activated balance. Once the bot finds a match, hackers use the gift card themselves or sell it on the "dark web."
RED FLAG: If you notice the balance of your gift card is gone, then contact the gift card issuer immediately.

WHAT TO DO: The best way to avoid this gift card scam is to simply use gift cards soon after you receive them, leaving little opportunity for a bot to find your gift card in the system.
I also suggest checking your unused gift card balances often. An easy way to do this is to load your plastic and egift cards into a gift card app or your smartphone's mobile wallet, both of which allow you to perform an automated balance inquiry. Lastly, if you have an unwanted gift card–one that you are not likely to use–then sell it for cash. People who buy discount gift cards are often planning to use them quickly so that is another way to ensure gift cards are used by their rightful owners.
For Merchants: Although I have heard it suggested that merchants prohibit balance check from their systems and instead require consumers to call a telephone number for balance inquiry to avoid this type of attack, I believe merchants should put security measures in place rather than inconveniencing consumers. Simple steps such as requiring a PIN or CVV in order to redeem a gift card or monitoring the number of balance inquiries that come into the system should help.
4. Stolen Card Number
HOW THE SCAM WORKS: In this scam, a thief removes a gift card from a display, records the number and then puts the gift card back in the display. Then the scammer waits for a customer to buy the compromised gift card, checking the balance online until a dollar amount is loaded onto the card. As soon as a balance appears, the thief uses the gift card number online or makes a duplicate plastic gift card that can be used in stores.
This gift card scam works best when there is a controlled number of gift cards available such as a small merchant with a stack of 10 gift cards on the counter. At a larger store, the gift cards near the cash register or on the ends of the rack would most likely be the ones affected.
RED FLAG: If someone tries to get you to purchase a particular gift card, it could be a scam. Pick a gift card from the middle of the rack or from a less-frequented area of the store.
WHAT TO DO: Since impatient thieves will put the gift cards they swiped back on the front of the rack, select gift cards that are less accessible. At a grocery store gift card kiosk, for example, you might select a card hanging in the middle position on one of the pegs rather than those that are hanging in the first position. In other words, don't be lured by the most obvious gift card on the rack.
5. Tampered Packaging
HOW THE SCAM WORKS: To protect consumers from the swiped gift card fraud described above, some gift card manufacturers have added special packaging or scratch-off personal identification numbers (PINs) to their cards to prevent thieves from being able to simply look at the cards to steal the gift card numbers. Though a deterrent, the packaging and PINs haven't fully stopped scammers. Some thieves will still take the packaged cards, open them to get the numbers, and then tidy the envelope back up in hopes no one will notice. Some also scratch off the PIN and re-cover it with a sticker or just leave it entirely exposed. Once the scammer has access to the gift card number, he or she will use it as soon as an unsuspecting customer activates the card.
RED FLAG: If the packaging looks tampered with in any way, it could be a scam. Check to see what other gift cards look like, inspecting the seams, PIN's and anything else that could be amiss.
WHAT TO DO: When buying a gift card, carefully check the packaging or PIN label. Don't just look for the obvious dismantling of a card, however. Scammers work hard to be discreet, using razor blades to separate the envelopes or scratch the PIN labels off with care. If the card looks tampered with in any way, turn it into the cashier and buy a different gift card.

6. Switched at Checkout

HOW THE SCAM WORKS: This gift card scam only works when a store employee is part of the plan. As the customer hands a gift card to the cashier for activation, the cashier activates a different card and hands the original back to the customer. (Or the opposite is true. The cashier activates the first card, but hands an inactive card to the customer.) In either case, the cashier racks up activated gift cards while handing out blanks.

RED FLAG: If the employee acts distracted or tries to distract you during gift card activation, it could be a scam. If the gift card number doesn't match the number on the activation receipt, this is also a problem.

WHAT TO DO: Keep your eye on the gift card at all times and ask to have it handed back to you as soon as the card is activated. Check the gift card number listed on the activation receipt to ensure it matches the number on the card you just received as well.

7. Discount Double-Dip

HOW THE SCAM WORKS: Thanks to the popularity of gift cards in general, there is a profitable gift card reseller market that consumers can use to sell their unwanted gift cards for cash or buy other gift cards for less than face value. To shorten the time between buying and selling these gift cards (and to eliminate the need to ship the physical plastics), many online resellers accept gift codes–the numbers on the cards–rather than require sellers to mail in their plastic gift cards before getting payment. Scammers sometimes try to sell their codes for cash, then quickly use the cards after the company confirms the balance and accepts the card. In some cases, the reseller will discover the fraud. In other cases, the person buying the discount gift card is the one who figures it out.

RED FLAG: If you purchase a discount gift card and find the balance is less than expected, it could be a scam.

WHAT TO DO: Only buy discount gift cards from resellers that provide a guarantee. While you may be able to get a bigger discount on a gift card sold via an individual using an online auction site or a "friend of a friend," you also run the risk of losing your money entirely if the seller has nefarious plans in place.