Gift Card Scams Explode in Upcoming Holiday Shopping Season

bolster.ai/blog/gift-card-scams-explode-in-upcoming-holiday-shopping-season/

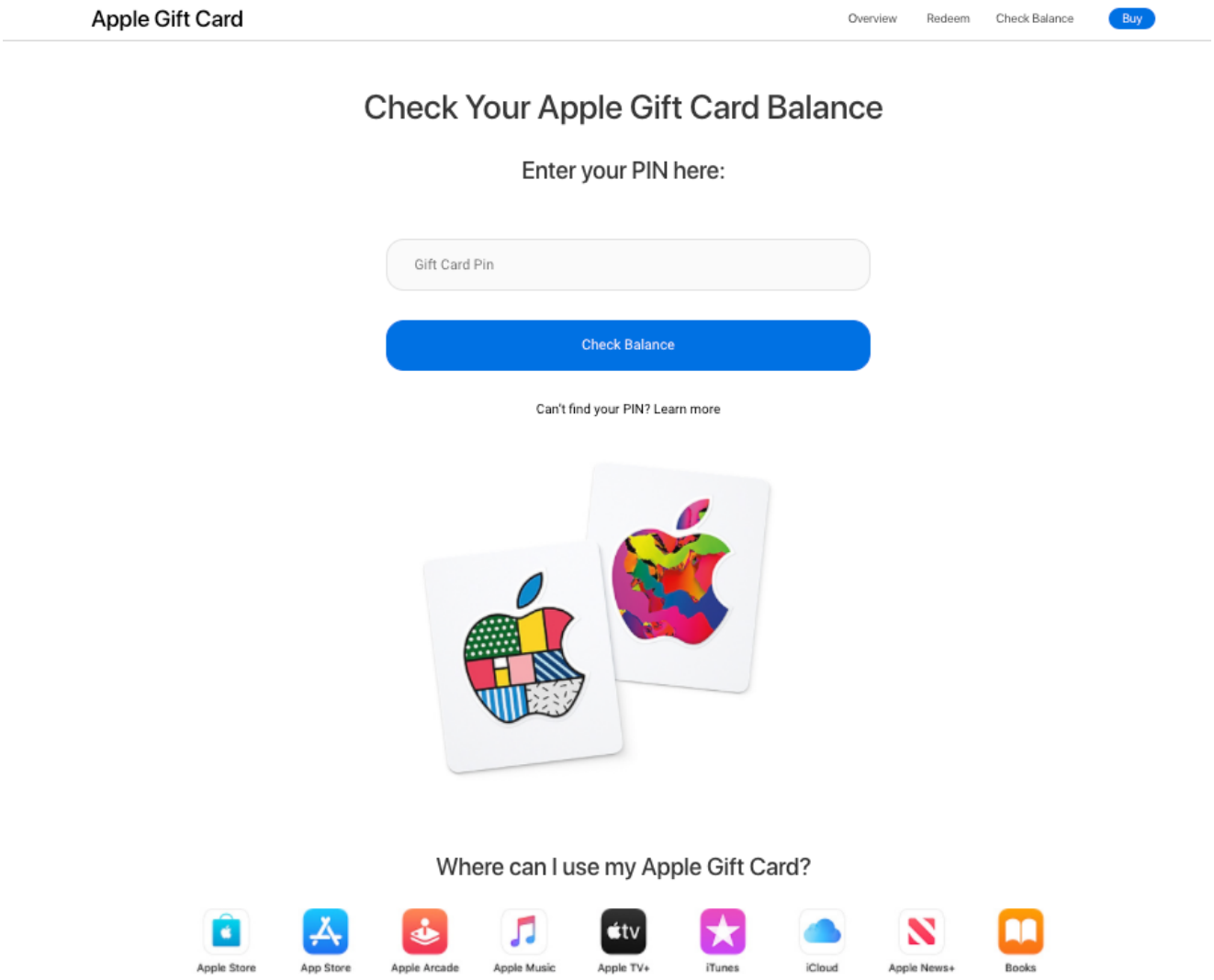
December 8, 2020 | 10 MIN READ

Update December 17, 2020

Gift card scams are continuing, and the criminals continue to target well-known Apple's new everything gift cards announced back in July. Instead of separate cards for iTunes or Apple Store purchases, consumers can now purchase a single gift card and use the to purchase products, accessories, games, music, movies, TV shows, iCloud, and more .

The site below leverages a typosquat attack and uses a URL that looks authentic and could easily fool somebody. The user is prompted to enter their gift card number to check their balance. Once they do, the site either hangs indefinitely or shows an error message. In some cases, it displays an invalid number message. Unfortunately for the user, if they get this far, it's already too late. The criminal has the gift card number and has either sold it on a gift card exchange or used it to make a purchase of their own.

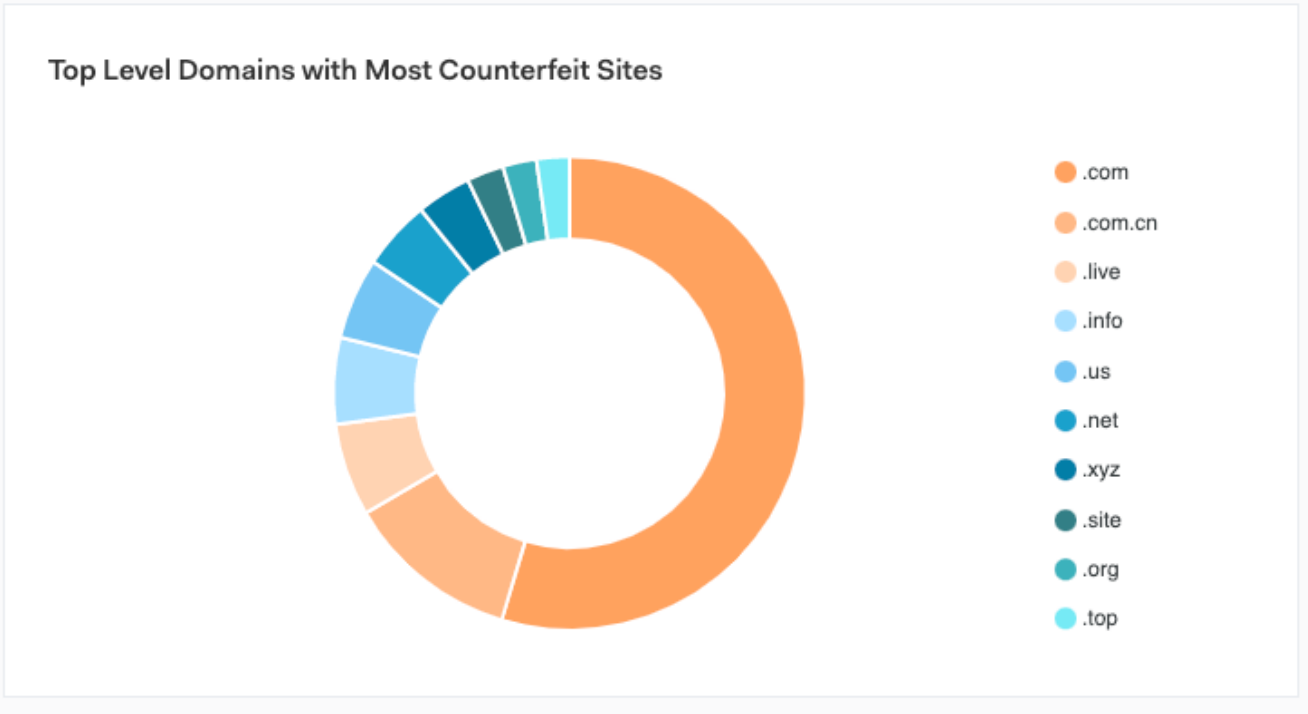
Scam Site URL: applegiftcardbalance[.]com



Apple Everything Gift Card Scam Site

Apple's new gift cards are likely to be a popular gift during this holiday season given the company's slate of new products launched this year. In the past 90 days, Bolster Research has found 1,645 phishing or scam Apple sites, and over 10,000 suspicious URLs that include the word "apple." The sites are hosted in multiple countries with some of the more interesting countries being the Russian Federation (588 sites), US Virgin Islands (75 sites), and Ukraine (2 sites).

The sites are hosted on a number of top level domains (TLDs), which demonstrates the problem companies face as more TLDs are created every year. The traditional defensive method of proactive domain registrations is economically unfeasible given that a six letter domain results in 1,200 variations. Bolster's has an extensive report and analysis of this problem, which can be read here.



Top Level Domains Hosting Apple Phishing/Scam Sites
Original blog post December 8, 2020

2020 has been an unpredictable year for retail and online shopping, and analysts are very cautious in their holiday season predictions The International Council of Shopping Centers (ICSC) predicts a nominal 1.9% increase from 2019(1), where Deloitte predicts two possible scenarios with retail holiday sales growth anywhere between 0% to 3.5%(2). Though the faltering economy, high unemployment and surging COVID-19 infections are causing anxious consumers to avoid brick and mortar stores, online shopping continues to rise.

Gift cards are one of most popular gifting options for the holidays, especially as e-gift cards are now available by most major retailers including Amazon, Target and Best Buy. Research firm Technavio forecasts a 13% compound annual growth rate for gift cards, driven by among other things the growth of e-commerce, which has exploded during the pandemic. Cyber criminals have taken notice and are launching specific online campaigns targeting gift cards.

Bolster research discovered a sharp rise in gift card scams as cyber criminals launch tactics to take advantage of the giving season. The analysis uncovered two primary types of gift card scams:

1. **Check your gift card balance**
   These sites offer to help you check the balance of your gift cards but steal gift card numbers from consumers.
2. **Survey scams with gift card offer**
   These sites offer bogus free gift cards for completing surveys, which are used to collect personal information which is sold for profit.

The data for this analysis was collected by the Bolster platform, which analyzes over one million sites daily and uses a combination of deep learning, natural language processing and computer vision to understand the intent of a site and make a determination whether it is a phishing or scam site. The technology has a false positive rate of 1/100,000.

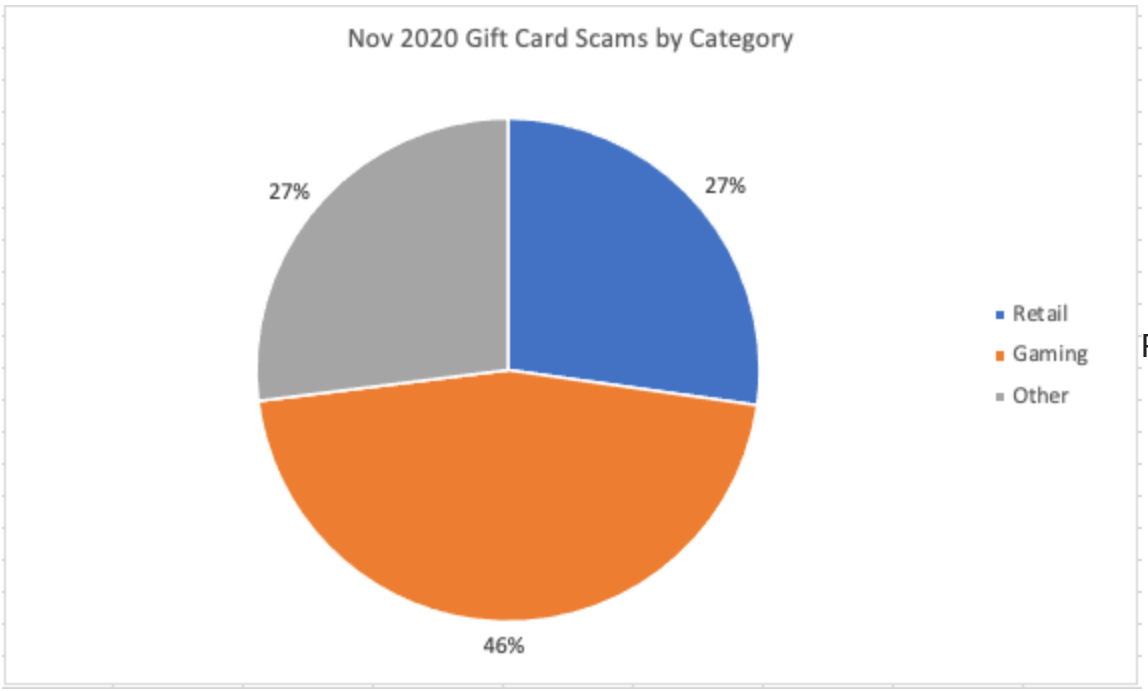
Gift Card Scams Explode

Bolster Research data shows that gift card scams first spiked in March and April as the COVID-19 pandemic caused many countries to issue shelter in place orders, corresponding with a sharp increase in e-commerce activity. After a brief lull in the summer, the data illustrates a more dramatic spike in September, which has continued into November. The large increase coincides with the early start of the holiday shopping season, including Amazon Prime Day in mid-October. November experienced the highest rate of new gift card scams with 6,881 total new sites, over 229 new sites per day and nearly 10X more new sites created than those in January.

Nearly 10X Increase in New Scams Monthly

Retail and Gaming are Prime Targets

Among the categories, retail and gaming are the most often targeted by gift card scammers going into the holiday season. In November, these two categories accounted for 59% of all gift card scams found online. The large increase is driven by the popularity of these categories during the holiday shopping season and the introduction of two highly anticipated new gaming consoles from Microsoft and Sony.

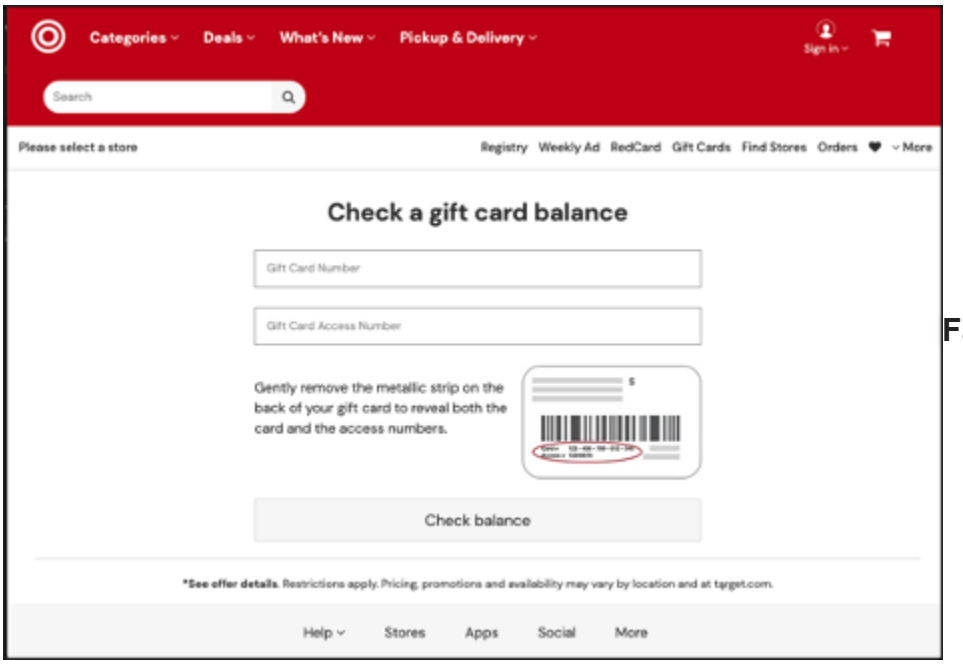


Percent of Gift Card Scams by Category

Check Your Gift Card Balance Scams

Target experienced a dramatic increase in e-commerce sales during the pandemic. In August, the company announced that its digital sales tripled with online purchases and curbside pickup jumped by more than 700%(3). Not surprisingly, Target gift cards are one of the more popular online scams discovered by Bolster Research.

The screenshot below illustrates a fraudulent Target gift card balance checker site. The layout, text and colors are identical to the authentic Target gift card balance checking site, which can be viewed here. Unsuspecting users can easily be tricked to enter their gift card numbers. Once they enter the number, the site displays a never ending “checking balance” status or some sort of error misleading users into thinking the site is malfunctioning. In reality, the valid gift card numbers are harvested by the criminals and monetized by either reselling them on other sites or using them to make purchases.



Fake Target Gift Card Balance Checker Site (https://www.targetgiftscard[.]com/)

Though the criminals went to a lot of effort to make this appear authentic, there are signs that this is not a legitimate Target site.

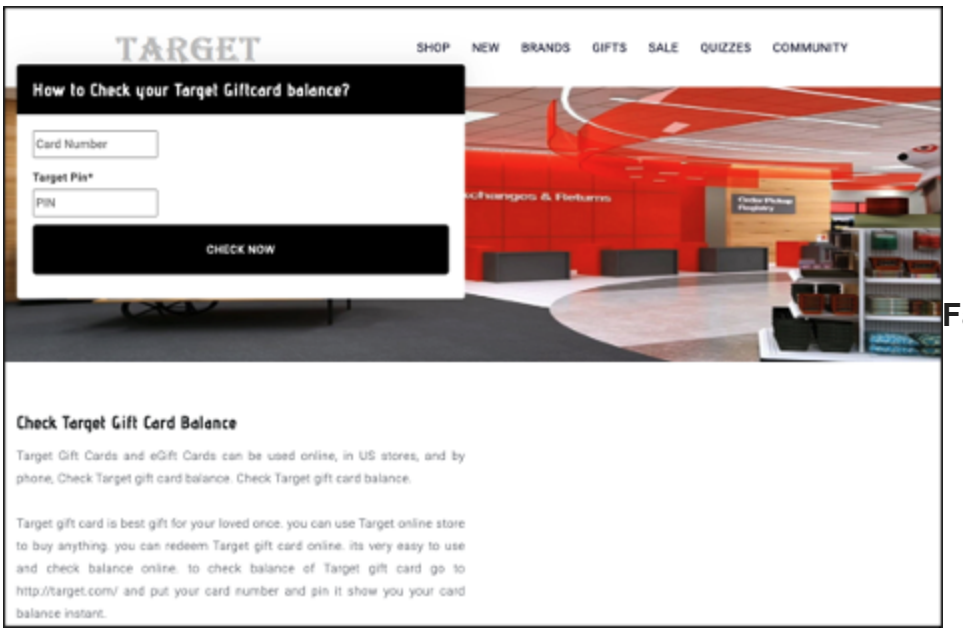
- **None of the other URLs work.** Clicking on the links to sign in, search store locations, or look at the weekly ads don't function. The reason is because criminals do not want their victims to leave the scam site. Linking to the real Target site would allow the users to go to leave the site before entering their gift card numbers.
- **The URL utilizes a typosquatting attack, utilizing a carefully chosen URL to trick users into believing it is an authentic Target site**. The wording is slightly awkward with "…giftScard.com" but this could be easily overlooked. Target does seem to own "…giftcard.com" and "…giftcards.com." These have been preemptively registered to prevent this type of attack. However, this scam site shows the limitations of preemptive domain registration as a defensive strategy. Bolster Research has an in-depth report that discusses the challenges of fighting typosquatting attacks and the limitations of preemptive domain registration.

More in-depth analysis, that would be typically beyond the technical abilities of the average consumer, confirms that this is not a legitimate Target site.

- **The domain is registered to an entity in the state of Delhi**, India. Target is a US-based company and would not register their domains in India.
- **The site is hosted in Singapore through GoDaddy.com.** GoDaddy is a consumer and small business service that is not used by large companies to host sites. Unless serving a foreign market, US companies host their sites in the US for the best user experience.
- **The IP address has been used for phishing sites in the past.** This data is available on Bolster's free community service Checkphish.ai.

- **The IP address is shared with other non-Target Indian business sites such as www.megabooster[.]in.** Large multinational corporations like Target use their own IP addresses and do not share them with other sites.

Bolster Research found other Target gift card scam sites that are less sophisticated and have a lower probability of tricking users. The official Target logos and colors are not used, and the text reads as the writer learned English as a second language. The main image looks like it is the inside of a Target store. What is interesting, however, is that by avoiding the use of Target's official logo, this site is more likely to evade detection. Most brand protection companies rely on the use of logos. Bolster discovered this site because its AI-driven platform combines highly accurate computer vision and natural language processing to assess the intent of the site, similar to how a human being would assess the site.



Fake Target Gift Card Balance Checker Site (http://etargetgift[.]com/)

Gift Card Survey Scam

Gift card survey scams are also becoming more prolific . These sites claim they can check for unused gift card codes. They offer these for free to users if they take the time to fill out a short survey. The purpose of these sites appears to be the collection of personal and demographic information that they will sell to companies or others that find this information useful.

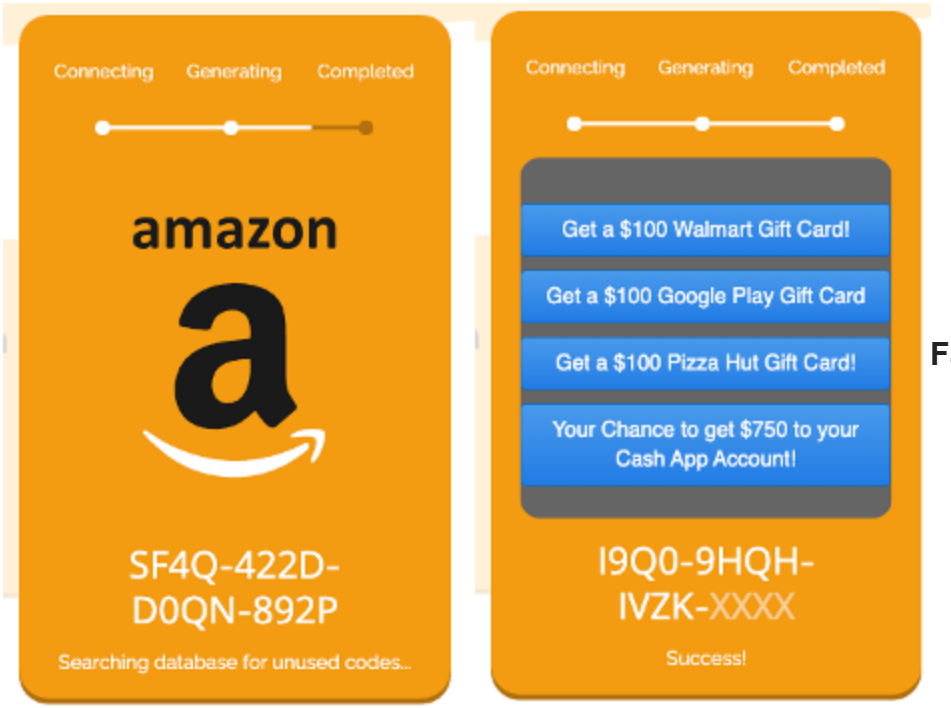
A single group looks to be behind hundreds of these scam sites using fake gift card offers from AliExpress, Bath & Body Works, Forever 21, and many others. The URL pattern is consistent and follows the template of https://[fake domain]/free-[brand name].html. For example, the URLs below are examples of fake survey sites that look and operate exactly the same except for the gift card brand being offered. Bolster Research has found more than 1,000 active survey scam sites that appear to be from the same perpetrator.

- https://liveoffer.online/free-aliexpress-gift-cards[.]html
- https://liveoffer.online/free-bathandbody-gift-cards[.]html
- https://gamer007.club/free-forever21-gift-cards[.]html
- https://wepromocode.com/free-amazon-gift-cards[.]html
- https://promohub.xyz/free-google-play-gift-cards[.]html
- http://real-giveaway.com/giftcard/free-hbo-gift-cards[.]html

Gift Card Survey Scam Site

(https://cardspace.club/free-amazon-gift-cards[.]html)

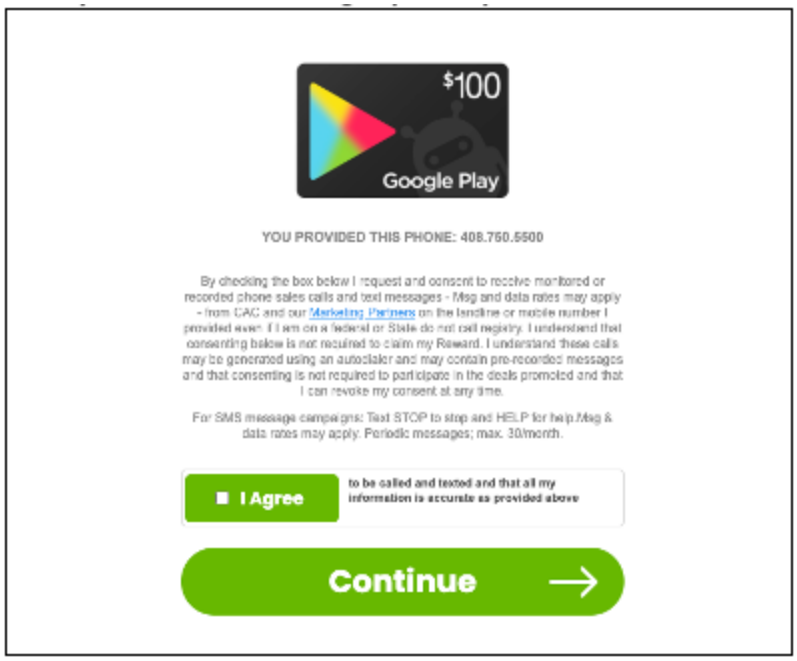
At face value, these survey scams seem overly simple. However, many people have lost their jobs or are struggling to survive financially, so it is not hard to imagine why people would fall for these scams. The scam site itself is very sophisticated and masterfully creates a sense of urgency to keep unsuspecting victims engaged. Once a gift card amount is selected, the site displays visuals designed to make the victim believe that a database search is occurring as in the screenshot below. The database search results in a success, and a partial gift card code is revealed.



Fake Amazon Gift Card

Scam Revealing Partial Codes

With the victim hooked, the site then proceeds to ask a series of survey questions to gather information such as name, address, phone number and date of birth. The survey continues to ask questions about spending habits, car insurance information, healthcare preferences, among other things. During the survey, the victim is required to explicitly opt-in to receive calls and text messages, even if they are listed on the federal or state do not call registry.

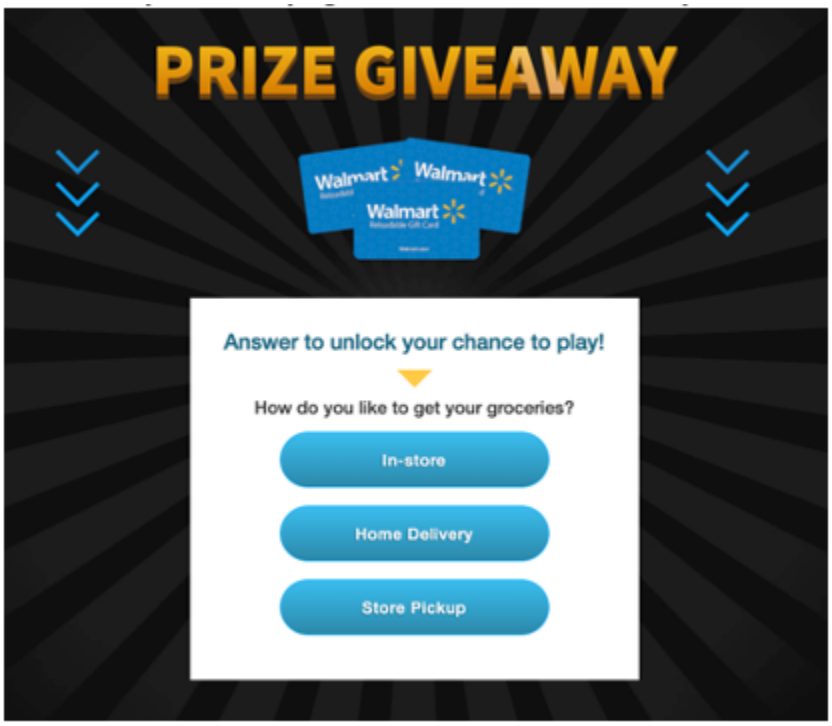


Survey Scam Site Obtaining

Explicit Opt-In Consent

Unfortunately for the user, there is no gift card at the end of the survey. What actually happens is an endless set of surveys that cover more and more preferences and demographic details. The victim is constantly encouraged to take one more survey for a

chance to win another gift card. It is obvious that the site was created by someone with an understanding of human psychology and gamification to encourage victims to reveal more and more personal information.



Fake Survey Site Notifying of Gift Card Prize Giveaway

How to Avoid Gift Card Scams

As cyber criminals ramp up gift card scams this holiday season, there is a good chance the average shopper will come across one of these campaigns. They could also receive a gift card as a present and unknowingly fall victim to one of these scams. Shoppers can stay save and avoid becoming a victim of these scams by following these helpful tips:

- **Always use the retailer's site to check gift card balances.** All retailers who offer gift cards have pages on their websites that allow shoppers to check gift card balances. Avoid checking your gift card balance on third party sites.
- **Go to a site by typing the retailer's URL directly.** Do not use a search engine such as Google to find a gift card balance checker page. Scammers are known to deploy search engine optimization tactics to rank high on search engine queries to lure unsuspecting victims. Using a search engine could cause you to go to a fake URL that closely resembles the real site.
- **Remember there are no free gift cards.** Though it is tempting to believe that today is your lucky day, nobody gives out free $50 gift cards for a few minutes of your time. The logic is impossible.

Bolster works with some of the largest brands to protect their users and customers from online phishing and fraud scams such as gift card scams. If you would like to learn more about how Bolster's AI platform can help you identify and remove gift card scams targeting your customers, please contact us.

Footnotes: