

# We Don't Want to Spoil Mother's Day but These Domains Might

## Table of Contents

1. [Executive Report](#)
2. [Appendix: Sample Mothers' Day-Related Domains and Subdomains](#)

## Executive Report

We're supposed to spoil our mothers on Mothers' Day, but with various scams out there, you may end up losing money or with a malware-infected device. WhoisXML API researchers found more than a thousand digital properties that could be used in Mothers' Day scams. Among our findings are:

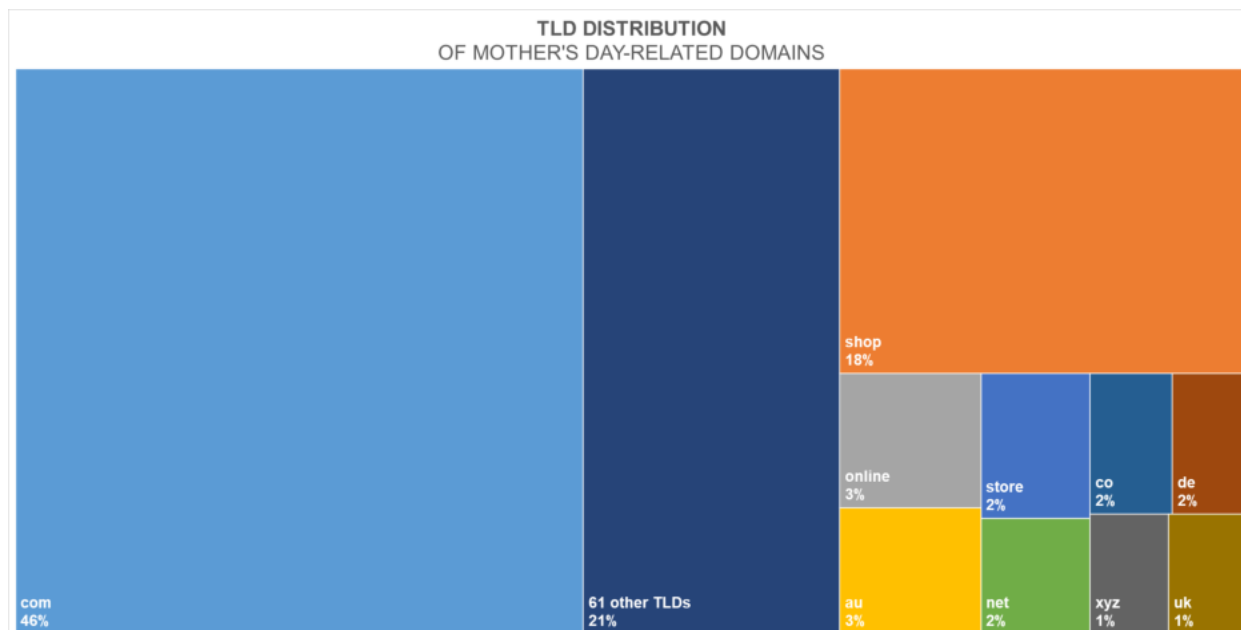
- 660+ domain names containing combinations of Mothers' Day-related text strings, such as "mother," "mom," "shop," "flower," "gift," "sale," and "card" added from 1 April to 3 May 2022
- 580+ subdomains containing the same text strings added within the same period
- Various malware engines flagged some of the web properties as malicious
- Some domains hosted suspicious content

## Analysis of Mothers' Day-Related Cyber Resources

### TLD Distribution

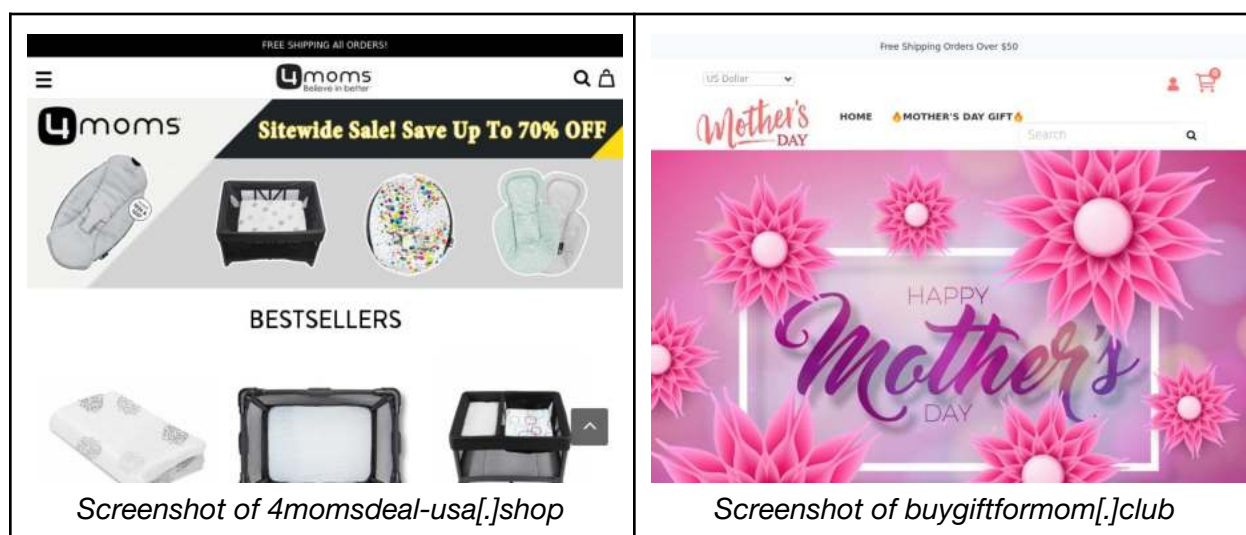
Almost half of the domains in the study fell under the .com top-level domain (TLD). Next to .com, other TLDs that stood out were e-commerce-related ones, such as .shop, .online, and .store. Country-code TLDs (ccTLDs) were also used repeatedly, including .au, .co, .de, and .uk. The rest of the domains were distributed across 60+ TLDs.

The chart below shows the TLD distribution of the Mother's Day-related domains added since 1 April 2022.



## Screenshot Analysis

Using [WhoisXML API's Screenshot API](#), we were able to find out more about the cyber resources. Several domains were, for instance, parked, while others hosted Mothers' Day-related content, mostly selling items targeting mothers. Some examples include:



Some of these websites certainly belong to legitimate small businesses that aim to make the most out of the event. However, some digital properties also hosted questionable content, including those that seem to impersonate Amazon and Walmart. Below are some examples.



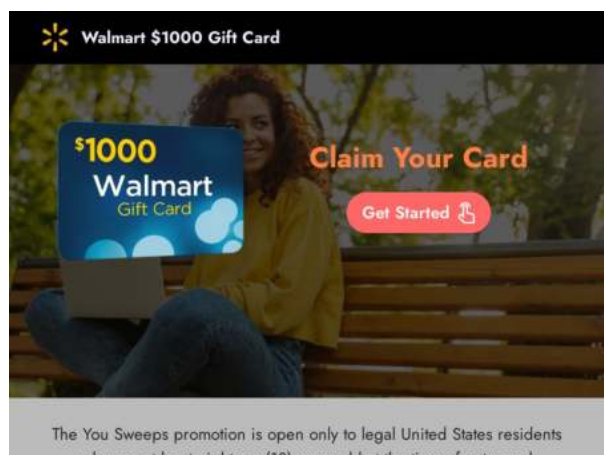
Screenshot of amazongiftcard[.]ml



Screenshot of freegetgiftcard[.]blogspot[.]com



Screenshot of giftcardfx[.]com



Screenshot of giftcwcad[.]us

Other concerning content looks like the login pages of email and social media platforms. This subdomain, for example, displays Google's login page.



One account. All of Google.

Sign in with your Google Account

A screenshot of the Google sign-in interface. It features a grey circular profile icon placeholder at the top. Below it is a white text input field with the placeholder text "Email or phone". Underneath the input field is a prominent blue button labeled "Next". To the right of the "Next" button, there is a smaller, grey text link that says "Find my account".

[Create account](#)

One Google Account for everything Google



*Screenshot of 1084-mothers-day-badge-2022[.]backstage[.]yellow[.]chordify[.]net*

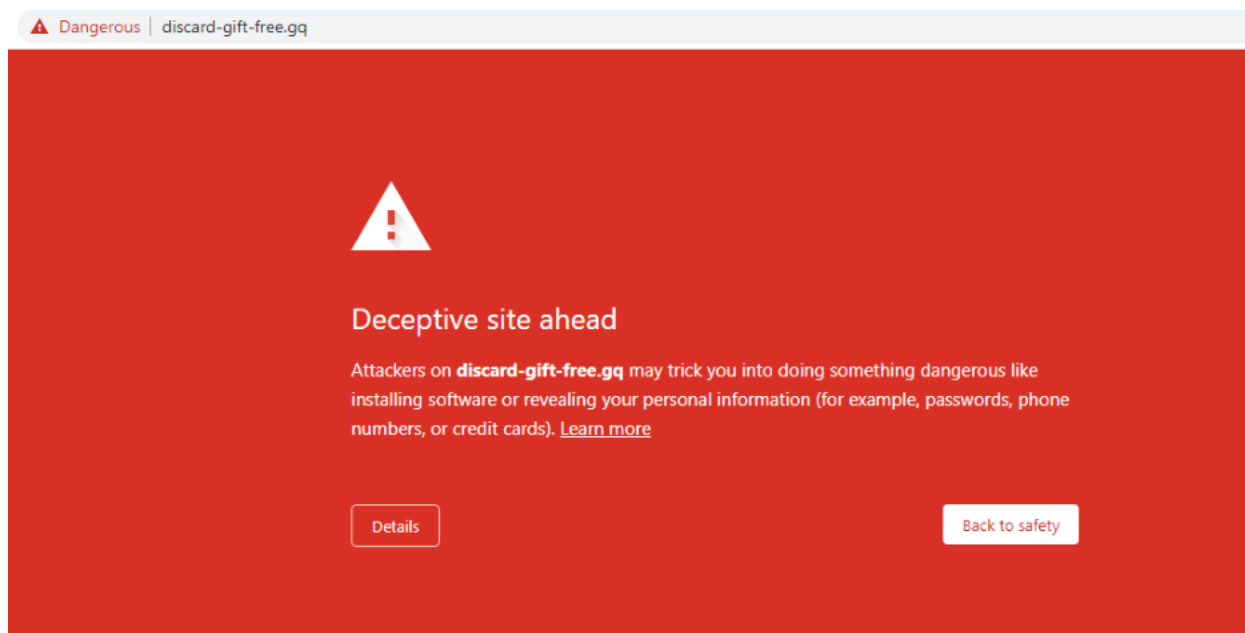
On the other hand, these gift card domains hosted Messenger login pages.

<p>A screenshot of a Messenger login page. At the top center is the Messenger logo. Below it, the text "Connect with your favorite people." is displayed. There are two input fields: "Email or phone number" and "Password". A blue "Continue" button is positioned below the input fields. At the bottom, there is a checkbox labeled "Keep me signed in". The footer contains links for "Not on Facebook?", "Forgot password", "Data Policy", "Terms", "Cookies Policy", and "© Meta 2022".</p> <p><i>Screenshot of coffeshopgiftcards[.]com</i></p>	<p>A screenshot of a Messenger login page, identical to the one on the left. It features the Messenger logo, the text "Connect with your favorite people.", input fields for "Email or phone number" and "Password", a blue "Continue" button, a "Keep me signed in" checkbox, and a footer with links for "Not on Facebook?", "Forgot password", "Data Policy", "Terms", "Cookies Policy", and "© Meta 2022".</p> <p><i>Screenshot of coffeshopgiftcards[.]com</i></p>
---	---

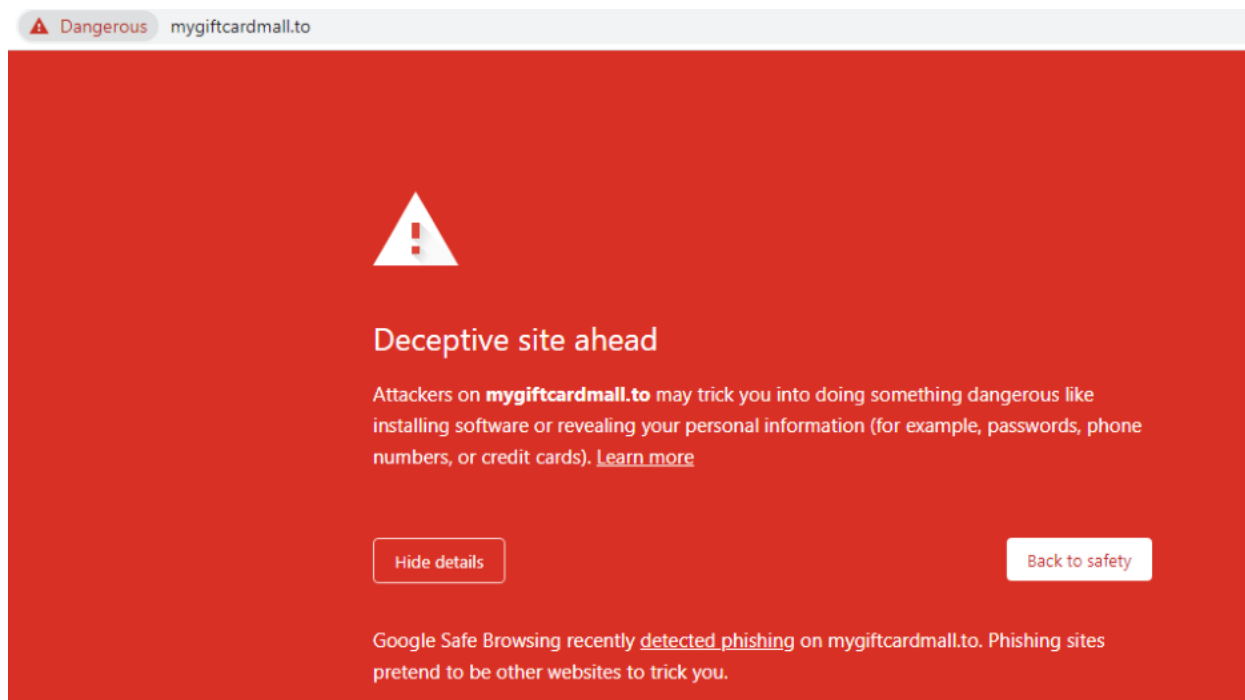


## Malware Check

Despite being just a little over a month old, some of the resources have already been flagged as malicious. More alarmingly, a few haven't been taken down. For instance, these domains seem to still resolve to deceptive sites.



*Screenshot of discard-gift-free[.gq]*





*Screenshot of mygiftcardmall[.]to*

People with weaker browser security may still fall victim to these websites.

## **Mothers' Day Scams the Web Properties May Enable**

More of the 1,200 domains and subdomains can be used maliciously in the coming days. Among the scams to look out for are described below.

### **Fake Gift Shops**

Phony online shops supposedly selling gifts and flowers for mothers may lure people in the weeks or days leading up to the event. Threat actors set up these digital stores and make them appear legitimate to steal the victims' financial information.

### **Fabricated Contests and Giveaways**

A [phishing campaign](#) targeting WhatsApp entices users with rewards, discounts, vouchers, and giveaways so they'd click malicious links. These links lead to fake Amazon pages that are set up to look legitimate, similar to those we found in our screenshot analysis above. Similar campaigns can be seen targeting email and social media platform users.

Aside from Amazon look-alike pages, our screenshot analysis also revealed several domains that hosted content congratulating visitors for winning gift cards or vouchers. If you didn't join any contest, this could be a sign of malicious activity.



# Congratulation

You Win \$1000 Amazon Gift Card!

To receive a gift from me, register your name now. Don't worry because registration is free. For android users you will be directed to the application (do download) and register there for free (this is mandatory).

Before the prize can be processed, Your registration is required! so you should complete your registration now.

Therefore, Prizes cannot be processed if you do not complete the registration stage.



Screenshot of [claim-now-gift-card1000blogspot\[.\]com](http://claim-now-gift-card1000blogspot[.]com)

## Malicious Electronic Cards

Threat actors may send electronic cards to mothers, posing as the victim's children. They may obtain the children's information from the mother's Facebook account, especially when email addresses and relationships are visible to the public. Using these details, threat actors can create email accounts using the children's names. Clicking the card would initiate malware installation on the victim's computer.

There are several ways to protect users from the malicious activities detailed above. This includes educating them about possible scams that target children who want to spoil their mothers with gifts.

On a higher level, monitoring domains in real-time and automating suspicious domain investigations through API calls can help nip these malicious campaigns in the bud.

***If you wish to perform a similar investigation or research, please don't hesitate to [contact us](#). We're always on the lookout for potential research collaborations.***



## Appendix: Sample Mothers' Day-Related Domains and Subdomains

### Sample Domains Related to Mothers' Day Added from 1 April to 3 May 2022

- motherdays[.]shop
- mothersdaybr[.]com
- mothersdaymx[.]com
- mothersdayfr[.]com
- mothersdayesp[.]com
- motherdayshop[.]com
- mothersdaygift[.]ca
- mothersday[.]jewelry
- graymothersday[.]xyz
- mothersdaysweet[.]com
- motherspeaceday[.]org
- motherdaygift[.]store
- fibeimothersday[.]com
- giftformother[.]club
- motherdaygift[.]store
- mothersdaygifts[.]life
- giftsformother[.]online
- mothers-day-gifts[.]co[.]uk
- motherland2022[.]com
- qicmothersday2022[.]com[.]au
- restoremothernature2022[.]org
- restoremothernature2022[.]net
- restoremothernature2022[.]com
- aomomo2022[.]com
- motherel[.]shop
- promother[.]shop
- motherful[.]shop
- motherenne[.]shop
- motherdays[.]shop
- motherhands[.]shop
- mothermudflower[.]farm
- motherflowercreative[.]com
- mothersdayflowerschicago[.]com
- chicagomothersdayflowerdelivery[.]com
- sunflowersapp[.]mom
- flowersformom[.]store
- giftcard[.]cr
- giftcard[.]ec
- cardgift[.]au
- giftto[.]cards
- giftcards[.]cr
- giftcards[.]ee
- working-sales-mother[.]com
- mothersdayplantsforsale[.]com
- shouldsmothercard[.]bar
- cardrightspendmother[.]rest
- mothersandmarketersnftcards[.]com
- momint[.]cards
- themomcard[.]life

### Sample Subdomains Related to Mothers' Day Added from 1 April to 3 May 2022

- mothersday[.]kami-photo[.]com
- mothersday[.]jitzrplace[.]com
- mothersday[.]thermaband[.]com
- mothersday[.]americanakitchenandbar[.]com
- mothersday[.]evolvenj[.]com





- mothersday[.]3rdstonehawaii[.]com
- mothersday[.]terryrdcommunitychurch[.]com
- mothersday[.]govtjobportal[.]online
- mothersday[.]pw[.]church
- mothersday[.]theliftgym[.]com
- giftformom[.]doribesty[.]com
- giftsformom[.]webspool[.]com
- www[.]theultimategiftformom[.]robca  
nyon[.]com
- mothersdaygiftcards[.]purlifemed[.]c  
om
- www[.]mothersdaygiftcards[.]purlife  
med[.]com
- mothersday2022[.]xlaser[.]club
- mothersday2022[.]rafstrengthandfitn  
ess[.]com
- mothersday2022[.]giftavibepremium[  
.]com
- mother-kfc-2022[.]iangreenland[.]uk
- mothers-day-2022[.]sammynicoleph  
otography[.]com
- mothers-day-2022[.]selahimage[.]co  
m
- www[.]mother-kfc-2022[.]iangreenla  
nd[.]uk
- www[.]mothers-day-2022[.]sammyni  
colephotography[.]com
- www[.]mothers-day-2022[.]selahima  
ge[.]com
- motherson-careers-2022-kgk9j1dm  
x-generous[.]vercel[.]app
- momk-shop[.]web[.]app
- momatshop[.]pages[.]art[.]br
- momeshopes[.]repl[.]co
- shopducmom[.]tsn1s[.]site
- momsdoishop[.]stockpotphotos[.]  
com
- mombela[.]shop[.]glossify[.]shop
- www[.]shopducmom[.]tsn1s[.]site
- giftcard[.]awapple[.]tokyo
- giftcard[.]sesoyr[.]com
- giftcard[.]upstairsatthegrill[.]co[.]uk
- giftcard[.]picturacreative[.]com[.]au
- giftcard[.]greenpay[.]com[.]bd
- giftcard[.]infinity[.]team
- momani-sales[.]myshopify[.]com
- mothersdaycontest[.]mayfloweronli  
ne[.]com
- mothersdaygiftcards[.]purlifemed[.]c  
om
- www[.]mothersdaygiftcards[.]purlife  
med[.]co
- cardamom[.]admin[.]id
- momocard[.]carrd[.]co
- cardamom[.]jeu[.]org
- cardamompet[.]xsrv[.]jp
- moment-cards[.]herokuapp[.]com
- www[.]cardamom[.]aicop[.]today
- dev3[.]cardamom[.]kidding[.]com

## Malicious Properties Flagged during the Malware Check Dated 3 May 2022

- sustainjubilantmother[.]shop
- whipwholesomemom[.]shop
- mygiftgiftcard-mall[.]com
- mygiftcardmall[.]to
- discard-gift-free[.]gq
- targetgiftbalancecardd[.]us
- cardamomh5lf[.]buzz
- grubomom2022[.]xxnnxx[.]org
- scintillating-sparkly-cardamom[.]glit  
ch[.]me