



Research Report on

“AMAZON INTERNATIONAL WOMEN’S DAY 2022 GIVEAWAY” SCAM



CyberPeace
—Foundation—

DISCLAIMER

This report is purely based on technical findings made by the research team during an investigation. It does not intend to malign or in any way target any country, actor or person. All the information provided in this report has been extracted during the investigation and information might be changed after generating the reports.

RESEARCH REPORT ON

“AMAZON INTERNATIONAL WOMEN’S DAY 2022 GIVEAWAY” SCAM

The Research Wing of CyberPeace Foundation received a link via Whatsapp related to a free giveaway campaign on the occasion of International Women’s day pretending to be an offer from Amazon which asks users to participate in a short quiz in order to get a chance to win 10,000 free gifts.



Link:

[https://tinyurl2\[.\]ru/m968834997/](https://tinyurl2[.]ru/m968834997/)

Case Study:

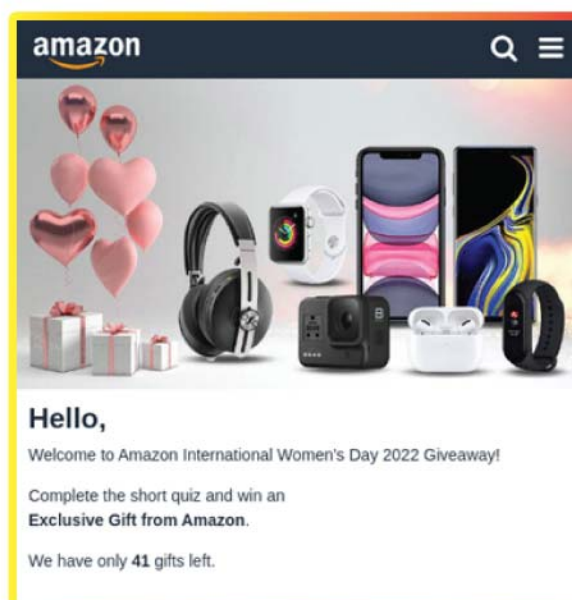
The Research Wing of CyberPeace Foundation along with Autobot Infosec Private Limited have looked into this matter to reach a conclusion that the website is either legitimate or an online fraud.

On Visiting the link users were redirected to

[https://tinyurl2\[.\]ru/m968834997/#XX](https://tinyurl2[.]ru/m968834997/#XX)

Where **XX represents a unique 13 digits number, for example **1633075913900**.

On the landing page a Welcome message appears with an attractive photo of Amazon products and asks users to participate in a short quiz in order to get Women’s Day gifts exclusively from amazon.



Also at the bottom of this page a section comes up which seems to be a social media comment section where many users have commented about how the offer is beneficial.

The quiz starts with some basic questions like **Do you know Amazon?**, **How old are you?**, **What you think about Amazon?**, **Would you recommend us to your friends?** Etc.



Question 1 of 4: Do you know Amazon?

YES

NO

Question 3 of 4: What you think about Amazon?

AMAZING

VERY GOOD

GOOD

NOT GOOD

Question 2 of 4: How old are you?

18-29

30-39

40-49

50+

Question 4 of 4: Would you recommend us to your friends?

YES

NO

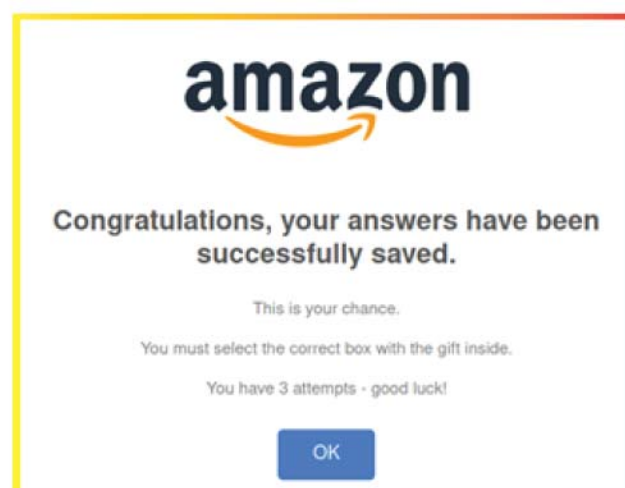
Once the user answers the questions a “congratulatory message” is displayed.

“Congratulations! your answers have been successfully saved.

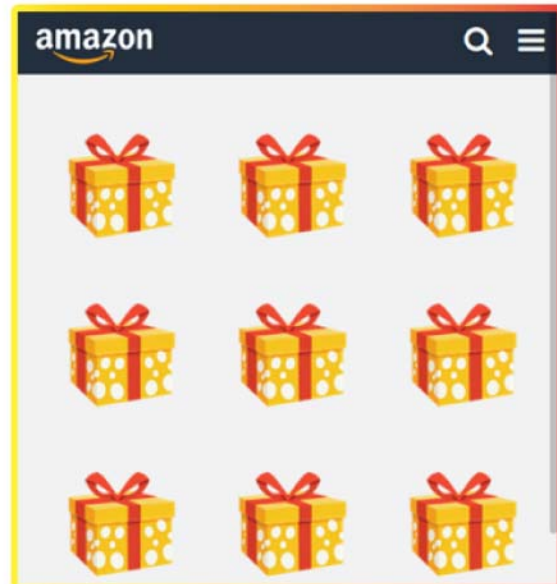
This is your chance.

You must select the correct box with the gift inside.

You have 3 attempts - good luck!”



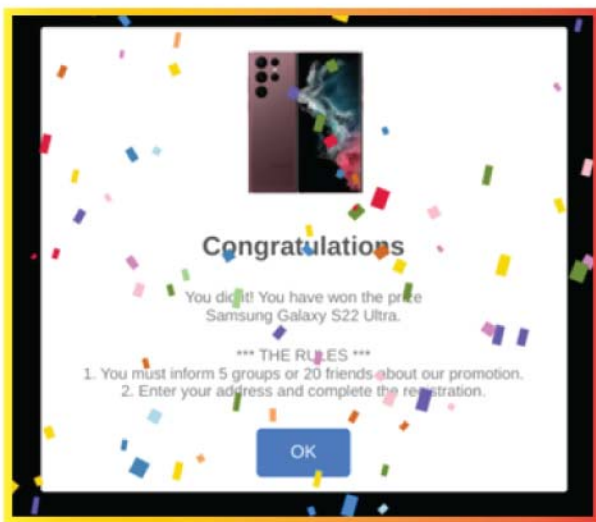
After Clicking the OK button users are given three attempts to win the prizes with multiple gift boxes.



After completing all the attempts it says that the user has won

“Congratulations!

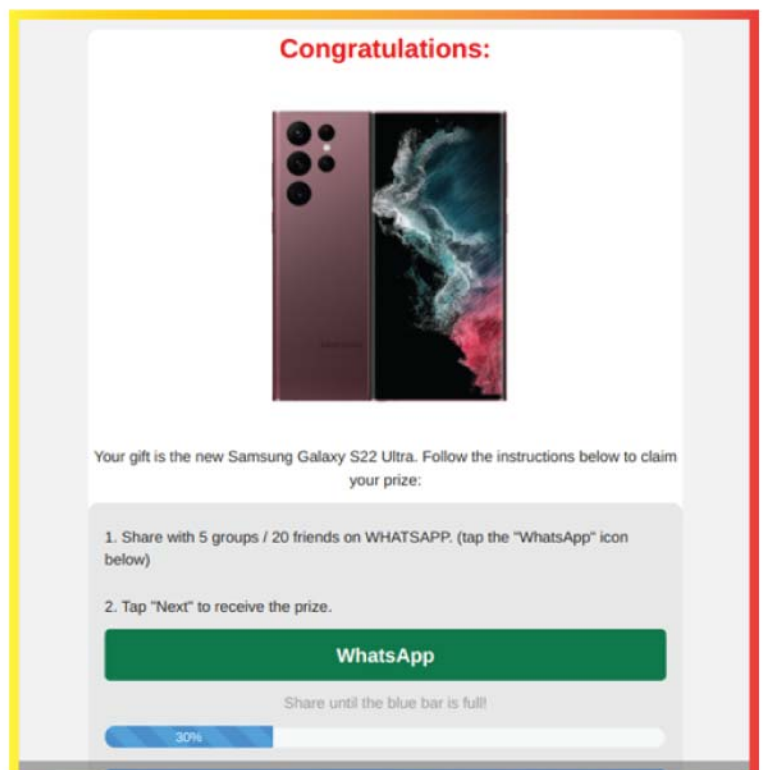
You did it! You have won the prize Samsung Galaxy S22 Ultra”



Clicking on the ‘OK’ button, it instructs users to share the campaign on WhatsApp.

Strangely enough the user has to keep clicking the WhatsApp button until the progress bar completes.

After clicking on the green ‘WhatsApp’ button multiple times it shows a section where instruction has been given in order to get the prize.



Your gift is the new Samsung Galaxy S22 Ultra. Follow the instructions below to claim your prize:

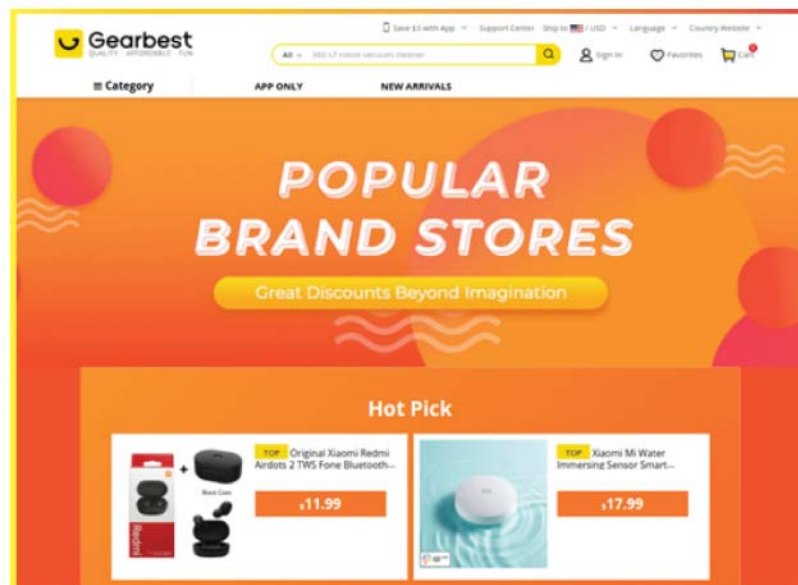
Very good! The last step:

1. You must complete the form to get your gift by clicking on "FINISH".

(Remember: This step is very important)

After completing the above instructions, wait for the administrator's review, which will be completed within 24 hours.

FINISH



On clicking the green FINISH button, it redirects the user to a promotional page of [gearbest\[.\]com](https://gearbest.com).



IN DEPTH INVESTIGATION :

Some of the key findings are as follows :

Domain Name	tinyurl2[.]ru
HTTP Status Code	200 [Active]
IP Address	188.114.96.0
ISP	Cloudflare
ASN	13335
Country	Colombia
Continent	South America

Whois Data :

domain: TINYURL2.RU
nserver: ishaan.ns.cloudflare.com.

nserver: mina.ns.cloudflare.com.
state: REGISTERED, DELEGATED, VERIFIED
person: Private Person
registrar: R01-RU
admin-contact: https://partner.r01.ru/contact_admin.khtml
created: 2022-01-30T12:16:48Z
paid-till: 2023-01-30T12:16:48Z
free-date: 2023-03-02
source: TCI

Last updated on 2022-03-03T05:21:30Z



HTTP RESPONSE HEADER

→ [https://tinyurl2\[.\]ru/m968834997/](https://tinyurl2[.]ru/m968834997/)

HTTP/1.1 200 OK

Date:	Thu, 03 Mar 2022 05:38:40 GMT
Content-Type:	text/html
Transfer-Encoding:	chunked
Connection:	close
Last-Modified:	Wed, 02 Mar 2022 14:15:49 GMT
Cache-Control:	max-age=14400
CF-Cache-Status:	MISS
Expect-CT:	max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Report-To:	{"endpoints":[{"url":"https://Va.nel.cloudflare.com/vreport/v3?s=9bzM0x%2FoX%2F0bZnMW2lcFhY1GXYoQsvZy%2FTdV1p1x23kclR0MeshyO2n0JX93mlgVFUpnJ0BFv7e4H8lCmfM9ACPp1g26ezDYiUqGJKkJZv%2B%2FvMvRelU2VNSSxFaqeA%3D%3D"}],"group":"cf-nel","max_age":604800}
NEL:	{"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server:	cloudflare
CF-RAY:	6e6006f658466f9e-IAD
alt-svc:	h3=":443"; ma=86400, h3-29=":443"; ma=86400

In source code analysis we found some information like –

- The title of the site is “Amazon International Women’s Day 2022 Giveaway”

```
<meta property="og:title" content="Amazon International Women's Day 2022 Giveaway">
<title>Amazon International Women's Day 2022 Giveaway</title>
<meta property="og:type" content="article">
```

- The section which seems to be a social media comment area is static and not a dynamic one. The section has been created with some HTML and CSS.

```
Carl Lewis
</p>
<p>
I received it today, thank you very much!
</p>
</div>
<div class="clr">
</div>
<div class="comment-status">
<span> Like · Comment 
<p>
I thought it was a scam, but it arrived this morning.
</p>
</div>
<div class="clr">
</div>
<div class="comment-status">
<span> Like · Comment <img src="https://i.imgur.com/T49rn98.png"
...

```

```
.name, .profile {
  cursor: pointer;
}

.name {
  font-weight: 700;
}

.comments_face {
  font-family: roboto, sans-serif;
  background: #fff;
}

.comments_face .comments {
  background: #eee;
  border-bottom: 2px solid #fff;
  padding: 10px;
}

.comments_face .profile {
  float: left;
  width: 60px;
  margin-right: 10px;
}

.comments_face .comment-content img, .comments_face .profile img {
  width: 100%;
}
```


- With the purpose of pushing the notification and tracking the user, Onesignal SDK has been used.

```
<script src="https://cdn.onesignal.com/sdks/OneSignalSDK.js"></script>
```

- In background analysis we found a site <https://settrogens.com> was being connected which may trigger the injection of other malware or unwanted programs.

URL: https://settrogens.com/link?z=4894105&var=global&yid={CLICK_ID}

```
for (t = 0; 10 > t; ++t) history.pushState({}, "", "#");
onpopstate = function (t) {
  t.state && location.replace("https://settrogens.com/link?z=4894105&var=global&yid={CLICK_ID}");
  //var myUrl = "https://tinyurl2.ru/w" + Math.random().toString().slice(2,11) + "/";
  //t.state && location.replace(myUrl)
}
```

Request :

```
🔗 Request to https://settrogens.com:443 [139.45.197.238]
GET /link?z=4894105&var=global&yid={CLICK_ID} HTTP/1.1
Host: settrogens.com
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96"
Sec-Ch-Ua-Mobile: ?1
Sec-Ch-Ua-Platform: "Android"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 5.0; SM-G900P Build/LPX2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```



■ Reponse :

🔒 Response from https://settrogens.com:443/link?z=4894105&var=global&yamid={CLICK_ID} [139.45.197.238]

```
HTTP/2 200 OK
Server: nginx
Date: Wed, 02 Mar 2022 04:45:39 GMT
Content-Type: text/html; charset=utf8
X-Trace-Id: 91b489fcec8dd19f19027fed63103aea
Link: <https://propeller-tracking.com>; rel="preconnect dns-prefetch",<https://my.rtmark.r
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: GET, POST, OPTIONS
Access-Control-Allow-Headers: Accept, Content-Type, Content-Length, Accept-Encoding
Access-Control-Max-Age: 86400
Pragma: no-cache
Cache-Control: no-transform, no-store, no-cache, must-revalidate, max-age=0
Expires: Tue, 11 Jan 1994 10:00:00 GMT
Timing-Allow-Origin: *
Set-Cookie: OAID=12aef064a04f40c487d6be9f6b2e880b; expires=Thu, 02 Mar 2023 04:45:39 GMT;
Set-Cookie: oaidts=1646196339; expires=Thu, 02 Mar 2023 04:45:39 GMT; path=/; secure; Same
Set-Cookie: syncedCookie=; expires=Tue, 10 Nov 2009 23:00:00 GMT
Set-Cookie: allcnt=1; expires=Thu, 02 Mar 2023 04:45:39 GMT
Strict-Transport-Security: max-age=1
X-Content-Type-Options: nosniff
Timing-Allow-Origin: *
```

- All the sections like quiz, winning prize, sharing features, blue progress bar present in the site are statically programmed.

```
<p class="result" id="result1">
You have answered all 4 questions
</p>
<p class="result" id="result2">
Your IP address is valid for this promotion
</p>
<p class="result" id="result3">
Gifts are available and in stock!
</p>
<h2> Congratulations, your answers have been successfully saved.
</h2>
<p>
This is your chance.
<br>
<br> You must select the correct box with the gift inside.
<br>
<br> You have 3 attempts - good luck!
</p>
<h2> Congratulations</h2>
<p> You did it! You have won the prize<br>Samsung Galaxy S22 Ultra.</p>
<br>
<p>*** THE RULES ***</p>
<p>1. You must inform 5 groups or 20 friends about our promotion.</p>
<p>2. Enter your address and complete the registration.</p>
<div id="p_modal_button3" class="p_modal_button" onclick="showShare();stopConf
```




CONCLUSIVE SUMMARY :

The campaign is pretended to be an offer from Amazon but hosted on the third party domain instead of the official website of Amazon which makes it more suspicious.

During the investigation we have noticed multiple redirections between the links.

We have investigated the URLs in a secured sandbox environment where the WhatsApp application was not installed. If any user opens the link from a device like smartphones where WhatsApp application is installed, the sharing features on the site will open the Whatsapp application on the device to share the link.

The prizes are kept really attractive to lure the laymen.

The domain used in the campaign has been registered recently.

During the investigation we noticed the link redirects the user to a 404 error page if the user opens the link in the desktop computer. However if the link gets opened on a mobile device the campaign works fine. It means cybercriminals have targeted mainly mobile internet users through this campaign.

Cybercriminals used Cloudflare technologies to mask the real IP addresses of the front end domain name used in the campaign.





CYBERPEACE ADVISORY :

CyberPeace Foundation and Autobot Infosec recommend that people should avoid opening such messages sent via social platforms.

If at all, user gets into this trap, it could lead to whole system compromise such as access to microphone, Camera, Text Messages, Contacts, Pictures, Videos, Banking Applications etc as well as financial losses.

Do not share confidential details like login credentials, banking information with such a type of scam.

Do not share or forward fake messages containing links without proper verification.

There is a need for International Cyber Cooperation between countries to bust the cyber-criminal gangs running the fraud campaigns affecting individuals and organizations, to make the Cyberspace resilient and peaceful.



ISSUED BY :

Research Wing, CyberPeace Foundation.

Research Wing, Autobot Infosec Private Limited.



www.cyberpeace.org | secretariat@cyberpeace.net