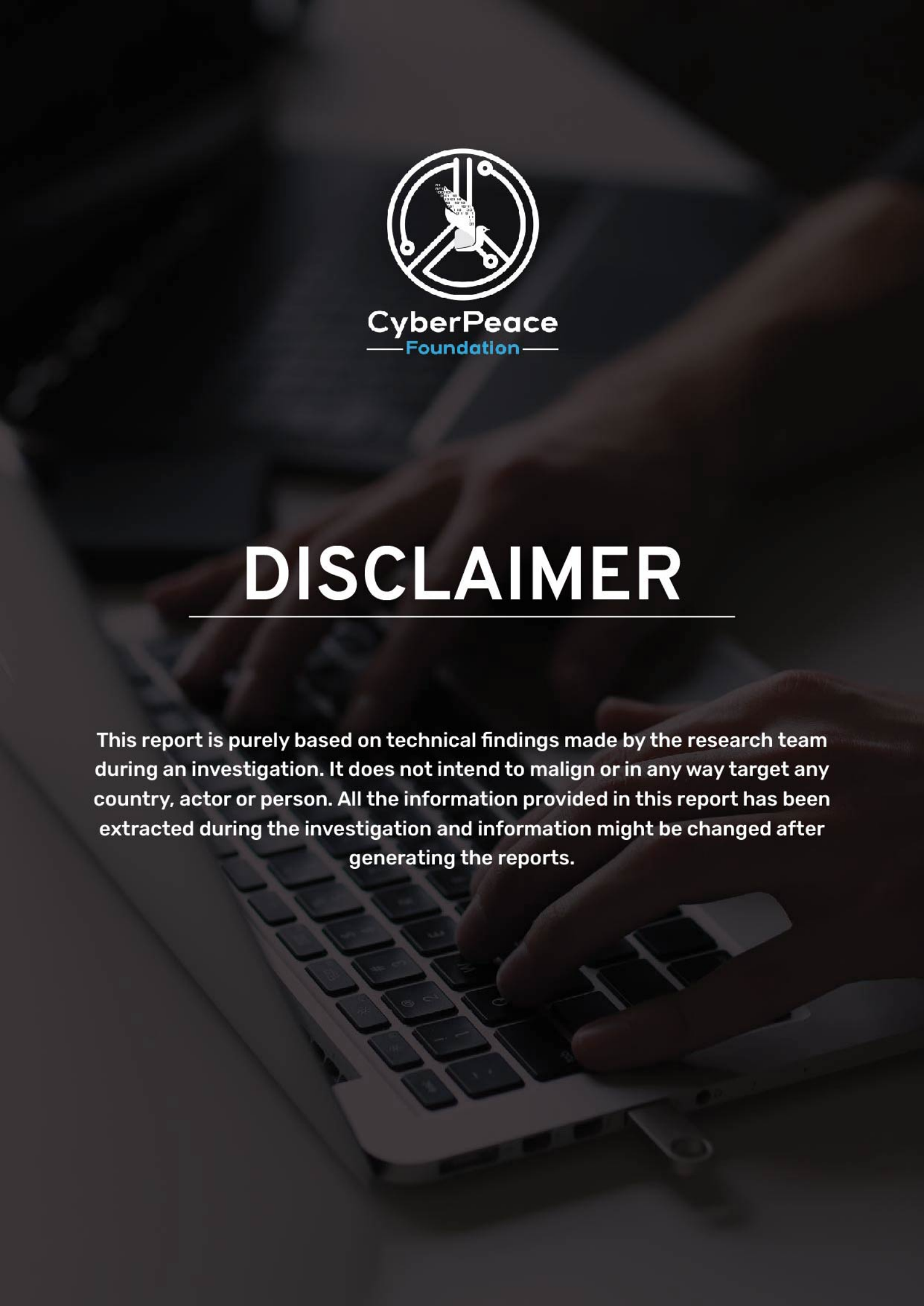
CyberPeace Foundation

Research Report on

CYBERCRIMINALS LURE INTERNET USERS TO GET INTO A MEDICAL SUBSIDY SCAM OF RS. 6000

WITH THE NAME OF APOLLO HOSPITAL



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

CYBERCRIMINALS LURE INTERNET USERS TO GET INTO A MEDICAL SUBSIDY SCAM OF RS. 6000 WITH THE NAME OF APOLLO HOSPITAL

The Research Wing of CyberPeace Foundation received a link via Whatsapp related to Apollo Hospitals Medical subsidy which asks users to click on the link and win 6000 rupees.

Link

http://gspnovh[.]cyou/ApolloHospitals-india/tb.php?gmqbajcu1659584547219

Summary

WARNING SIGNS

- The campaign is pretended to be an offer from Apollo Hospital but is hosted on the third-party domain instead of the official Apollo Hospital website which makes it more suspicious.
- The domain names associated with the campaign have been registered in very recent times.
- Multiple redirections have been noticed between the links.
- No reputed site would ask its users to share the campaign on WhatsApp.
- The prize is kept really attractive to lure the laymen.
- Grammatical mistakes have been noticed.

CYBERPEACE ADVISORY

- CyberPeace Foundation recommends that people should avoid opening such messages sent via social platforms.
- Falling into this trap could lead to whole system compromise such as access to the microphone, Camera, Text Messages, Contacts, Pictures, Videos, Banking Applications, etc as well as the financial loss for the users.
- Do not share confidential details like login credentials, and banking information with such a type of scam.
- Never share or forward fake messages containing links to any social platform without proper verification.
- There is a need for International Cyber Cooperation between countries to bust the criminal gangs running fraud campaigns affecting individuals and organisations to make Cyberspace resilient and peaceful.

Case Study

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

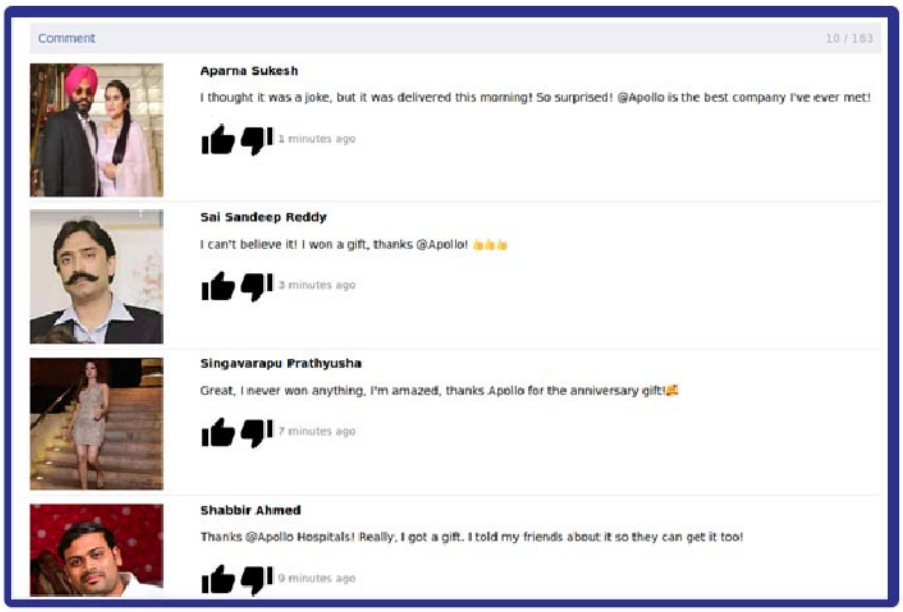
On Visiting the link users were redirected to

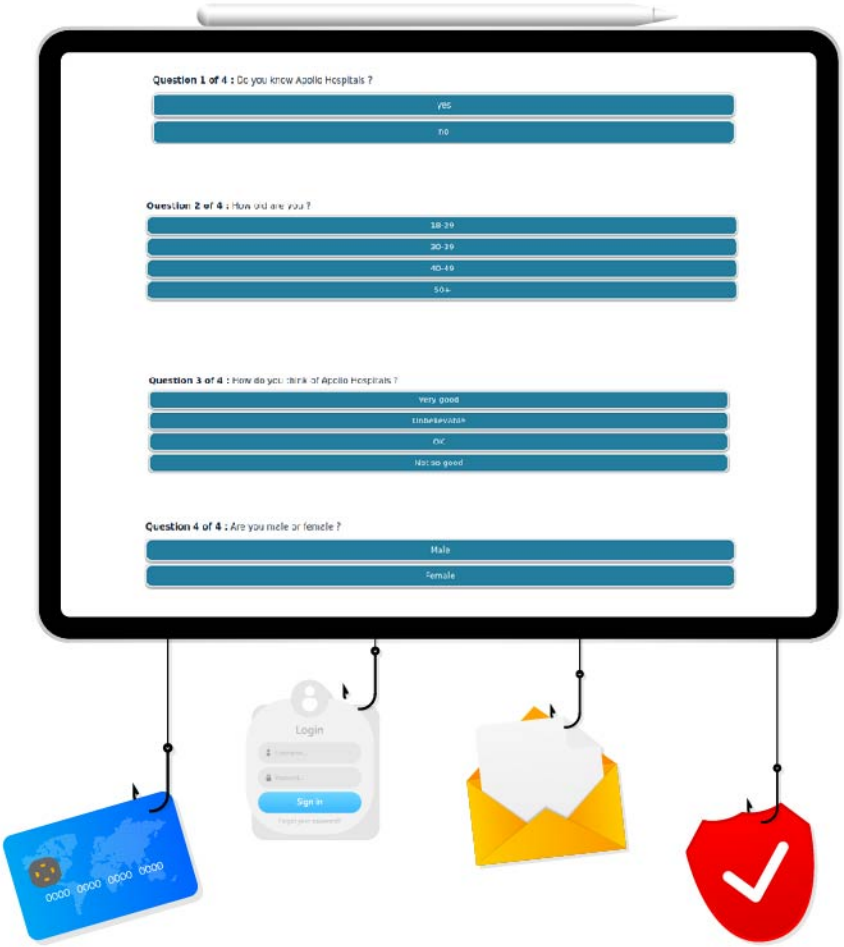
https://upceshop.cn/XF8yZiK2/ApolloHospitals-india/?_t=1659720746024#XX

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

On the landing page, there is an image of Prathap C. Reddy (founder of Apollo) and a message that says (Through the questionnaire, you will have a chance to get 6000 rupees).

At the bottom of this page, there is a section that seems like a social-media comment section.





The user has to answer four questions to win a price of 6000 rupees. It starts with some basic questions like -

“Do you know Apollo Hospitals?

How old are you?

How do you think of Apollo Hospitals?

Are you male or female?” etc.

After answering all four questions a congratulatory message appears.

“Congratulation!

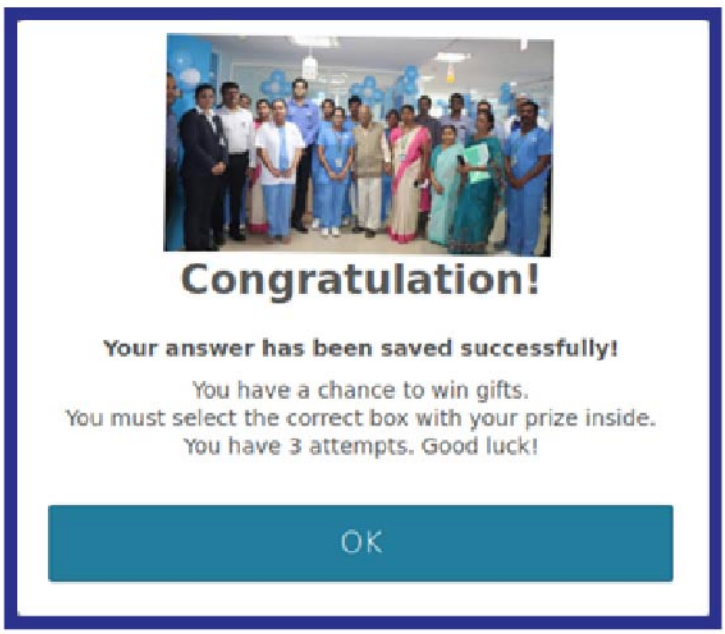
Your answer has been saved successfully!

You have a chance to win gifts.

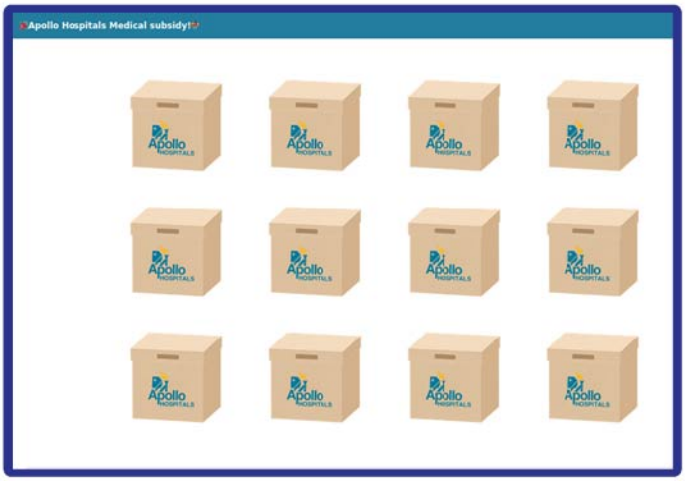
You must select the correct box with your prize inside.

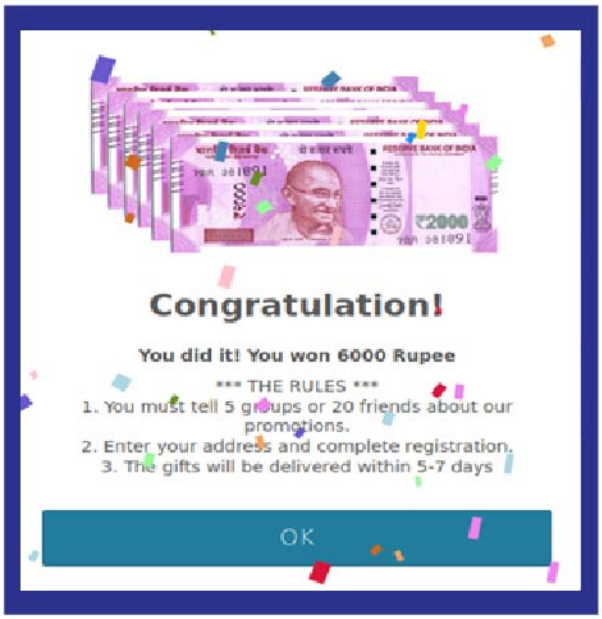
You have 3 attempts. Good luck!”

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



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





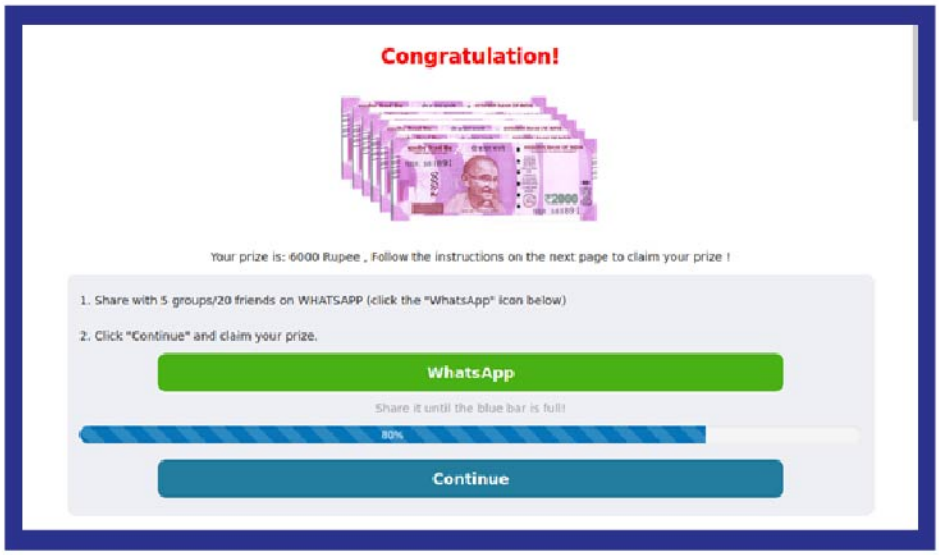
On the 2nd attempt, it says that the user has won a Gift card worth 6000 rupees.

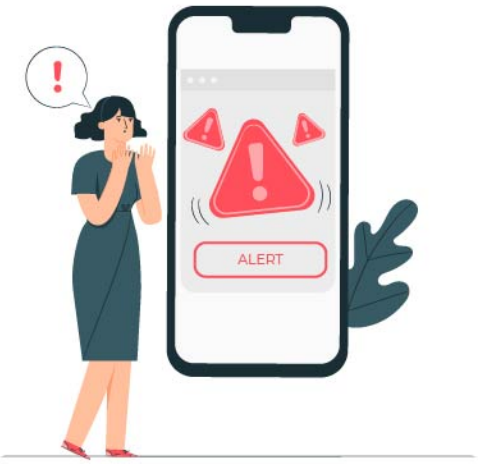
“Congratulation!

You did it! You won 6000 Rupee”

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

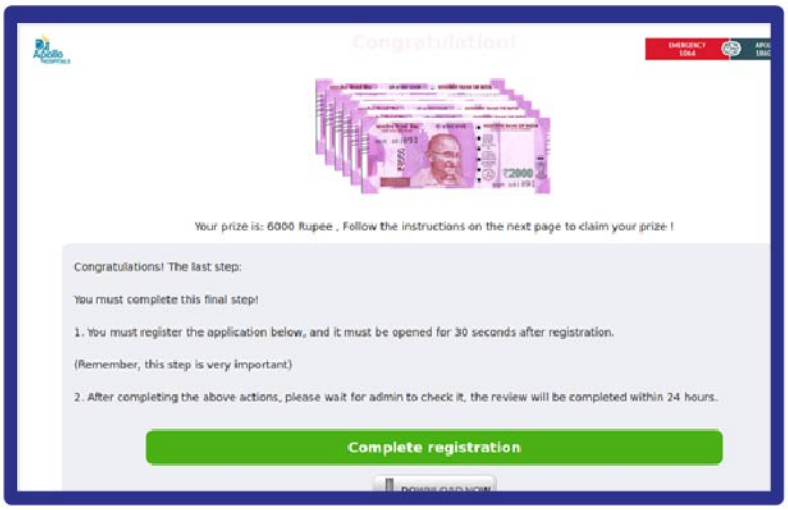
Clicking on the ‘OK’ button, it instructs users to share the campaign on WhatsApp, strangely enough, the user has to click the WhatsApp button until the blue bar reaches 100%.





After clicking the Continue button, a new box appears, here the user has to complete registration according to the given steps.

When the user clicks on the Complete registration button it redirects users to multiple advertisement pages and it varies every time the user visits the URL.



IN DEPTH INVESTIGATION :

Some of the key findings are as follows :

Domain Name	gspnovh[.]cyou
HTTP Status Code	200 [OK]
IP Address	172.67.182.206
ISP	Cloudflare
ASN	13335
Country	China
Continent	Asia

Domain Name: gspnovh.cyou

Registrar URL: http://www.hkdns.hk

Registrar: West263 International Limited

Registrar IANA ID: 1915

Updated Date: 2022-07-20T04:25:56.0Z
Creation Date: 2022-02-11T08:58:12.0Z
Registry Expiry Date: 2023-02-11T23:59:59.0Z

Registrant State/Province: Bei Jing Shi
Registrant Country: CN (China)

Name Server: GABRIELLA.NS.CLOUDFLARE.COM
Name Server: NICOLAS.NS.CLOUDFLARE.COM

Domain Name	upceshop[.]cn
HTTP Status Code	200 [OK]
IP Address	104.21.59.190
ISP	Cloud flare
ASN	13335
Country	China
Continent	Asia

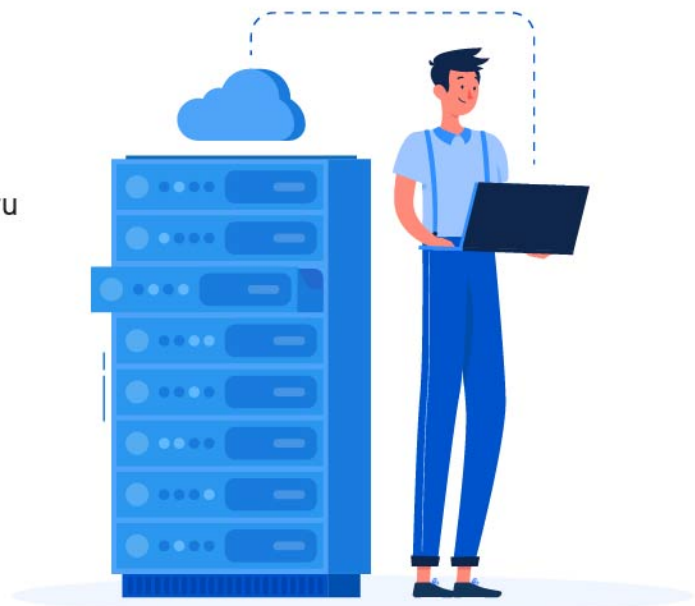
Domain Name: upceshop.cn
ROID: 20220717s10001s48552900-cn
Domain Status: ok

Registration Time: 2022-07-17 19:11:18
Expiration Time: 2023-07-17 19:11:18

Registrant: 刘甜甜 (Liu Tiantian)
Registrant Contact Email: evgeniyapbn5gle@mail.ru

Sponsoring Registrar: 阿里云☒算有限公司 (万网
[Alibaba Cloud Computing Co., Ltd. (Wanwang)]

Name Server: raegan.ns.cloudflare.com
Name Server: maxim.ns.cloudflare.com



In source code analysis we found some information like –

- The title of the page is “Apollo Hospitals Medical subsidy!

```
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>🎉Apollo Hospitals Medical subs
idy! 🎁 </title>
<meta property="og:title" content="🎉Apollo Hospitals Medical subsidy!🎁">
<meta property="og:description" content="🎁Medicaid is available to every citizen!💝">
<meta property="og:image" itemprop="image" content="https://263cdn.com/upload/ApolloHos
<meta property="og:url" content="https://www.apollohospitals.com/">
<meta property="og:type" content="website">
```

- We found three Google tag manager Ids **(G-HZ2ZQY399T, G-LW7434MYMN, G-0C230YDF7G)** in the source code.

```
599    <script aria-hidden="">
600        window.dataLayer = window.dataLayer || [];
601        function gtag(){dataLayer.push(arguments);}
602        gtag('js', new Date());
603        gtag('config', 'G-HZ2ZQY399T');
604    </script>
```

```
242 <script aria-hidden="true">
243   window.dataLayer = window.dataLayer || [];
244   function gtag(){dataLayer.push(arguments);}
245   gtag('js', new Date());
246
247   gtag('config', 'G-LW7434MYMN');
248 </script><script async="" src="%F0%9F%8E%89%EF%B8%8F%EF%B8%8F%F0%9F
```

```
!49 <script aria-hidden="true">
!50   window.dataLayer = window.dataLayer || [];
!51   function gtag(){dataLayer.push(arguments);}
!52   gtag('js', new Date());
!53
!54   gtag('config', 'G-0C230YDF7G')
```

```
1  GET /gtag/js?id=G-LW7434MYMN HTTP/1.1
2  Host: www.googletagmanager.com
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4  Accept: */*
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Referer: https://upceshop.cn/
8  Sec-Fetch-Dest: script
9  Sec-Fetch-Mode: no-cors
10 Sec-Fetch-Site: cross-site
11 Te: trailers
12 Connection: close
13
```

```
GET /gtag/js?id=G-HZ2ZQY399T HTTP/1.1
Host: www.googletagmanager.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://upceshop.cn/
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: cross-site
Te: trailers
Connection: close
```

```
GET /gtag/js?id=G-0C230YDF7G HTTP/1.1
Host: www.googletagmanager.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://upceshop.cn/
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: cross-site
Te: trailers
Connection: close
```

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.

Users are insisted on sharing the campaign with WhatsApp friends and groups.

```
    }
    location.href = 'whatsapp://send?text=' + jurl + new Date().getTime();
    setTimeout(function() {
        get_Cookie('prog') == '' ? value = 1 : value = parseInt(get_Cookie('prog'));
        if (value >= g_share_step) {
            continueBtn();
        } else {
            value == 2 || value == 4 ? swalert("The same group or the same friend is not correct. Please check and share again.",
                "Sharing failed!") : void(0);
        }
        set_Cookie('prog', value + 1);
```

In background analysis we found that this website is sending requests to other domains like-

uprimp.com

qoaaa.com

```
GET /bnr.php?section=General&pub=593174&format=300x50&ga=g HTTP/1.1
Host: uprimp.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://upceshop.cn/
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: cross-site
Te: trailers
Connection: close
```

```
GET //4fe48aebd6/4f59451604/?placementName=Flow&randomA=0_4550&maxw=0 HTTP/2
Host: qoaaa.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://upceshop.cn/ih3kOYjv/ApolloHospitals-india/?_t=1659897281474
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Te: trailers
```

We found some Chinese language written in the source code.

```
function getMainHost() {
    // 获取主域名
    let key  = `mh_${Math.random()}`;
    let keyR = new RegExp( `(^|;)\\s*${key}=12345` );
    let expiredTime = new Date( 0 );
    let domain = document.domain;
```

In source code analysis we found some javascript functions that collect the browser and system information from the user's device.

```
function getBrowser() {
    if ((navigator.userAgent.indexOf("Opera") || navigator.userAgent.indexOf("OPR")) != -1) {
        return "Opera";
    } else {
        if (navigator.userAgent.indexOf("Chrome") != -1) {
            return "Google Chrome";
        } else {
            if (navigator.userAgent.indexOf("Safari") != -1) {
                return "Safari";
```

```
function getPlatform() {
    if (window.navigator.userAgent.indexOf("Windows NT 10.0") != -1) {
        return "Windows 10";
    }
    if (window.navigator.userAgent.indexOf("Windows NT 6.2") != -1) {
        return "Windows 8";
    }
    if (window.navigator.userAgent.indexOf("Windows NT 6.1") != -1) {
        return "Windows 7";
```

****Important****

During the analysis, we found some javascript code in the background called hm.js was being executed from the host (**hm.baidu.com**) which is a subdomain of Baidu and is used for Baidu Analytics, also known as Baidu Tongji.

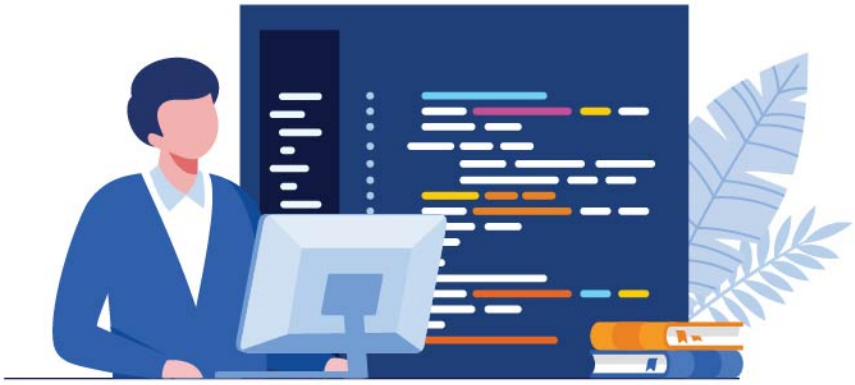
Note: "Baidu is a Chinese multinational technology company specializing in Internet Related services, products, and artificial intelligence, headquartered in Beijing's Haidan district, China."

```
        var _hmt = _hmt || [];
        (function() {
            var hm = document.createElement("script");
            hm.src = "https://hm.baidu.com/hm.js?bbb3e86814c9ceef66d180a6c15fa17d";
            var s = document.getElementsByTagName("script")[0];
            s.parentNode.insertBefore(hm, s);
        })();
        var _hmt = _hmt || [];
        (function() {
            var hm = document.createElement("script");
            hm.src = "https://hm.baidu.com/hm.js?14023b72d60769772946d154adb8f350";
            var s = document.getElementsByTagName("script")[0];
            s.parentNode.insertBefore(hm, s);
        })();
        var _hmt = _hmt || [];
        (function() {
            var hm = document.createElement("script");
            hm.src = "https://hm.baidu.com/hm.js?8b68846a3ac1709b0ec7199084ee5ea8";
            var s = document.getElementsByTagName("script")[0];
            s.parentNode.insertBefore(hm, s);
        })();
    </script>
```

```
</html><script>
    var _hmt = _hmt || [];
    (function() {
        var hm = document.createElement("script");
        hm.src = "https://hm.baidu.com/hm.js?70f5f07b8105f501ec0a2de78be68631";
        var s = document.getElementsByTagName("script")[0];
        s.parentNode.insertBefore(hm, s);
    })();
</script>
```

```
GET /hm.js?14023b72d60769772946d154adb8f350 HTTP/1.1
Host: hm.baidu.com
Cookie: HMACCOUNT=84811DBE3DDCB324; HMACCOUNT_BFESS=84811DBE3DDCB324
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://upceshop.cn/
Sec-Fetch-Dest: script
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: cross-site
Te: trailers
Connection: close

```



Domain Name	hm.baidu.com
HTTP Status Code	200 [OK]
IP Address	103.235.46.191
ISP	Baidu (Hong Kong)
ASN	555967
Country	Hong Kong
Continent	Asia

Domain Name: baidu.com
Registry Domain ID: 11181110_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292

Updated Date: 2022-01-25T09:23:56+0000
Creation Date: 1999-10-11T11:05:17+0000
Registrar Registration Expiration Date: 2026-1011T07:00:00+0000

Registrant Organization: Beijing Baidu Netcom Science Technology Co., Ltd.
Registrant State/Province: Beijing
Registrant Country: CN (China)

CONCLUSIVE SUMMARY :

- The campaign is pretended to be an offer from Apollo Hospital but hosted on the third-party domain instead of the official website of Apollo Hospital 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 a smartphone where the 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.
- Both the domain names used in this campaign have the registrant country as China.
- The domain names associated with the campaign have been registered in very recent times.
- Cybercriminals used Cloudflare technologies to mask the real IP addresses of the front-end domain names used in this gift scam campaign. But during the phases of the investigation, we have identified a domain name that was requested in the background and has been traced as belonging to China.

CYBERPEACE ADVISORY :

- CyberPeace Foundation and Autobot Infosec recommend that people should avoid opening such messages sent via social platforms.
- If at all, the user gets into this trap, it could lead to a whole system compromise such as access to the microphone, Camera, Text Messages, Contacts, Pictures, Videos, Banking Applications, etc as well as financial losses.
- Do not share confidential details like login credentials, or 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 organisations, to make Cyberspace resilient and peaceful.

ISSUED BY :

Research Wing, CyberPeace Foundation.

Research Wing, Autobot Infosec Private Limited.

www.cyberpeace.org | secretariat@cyberpeace.net

/cyberpeacefoundation /cyberpeacengo /cyberpeacefoundation