

# Shared content spoofing based on OG (Open Graph) protocol forgery

## Description

Apple's Messages app supports the parsing of shared links and displays them in the form of title and image, allowing users to get a preview of the content (shown in Figure 1).

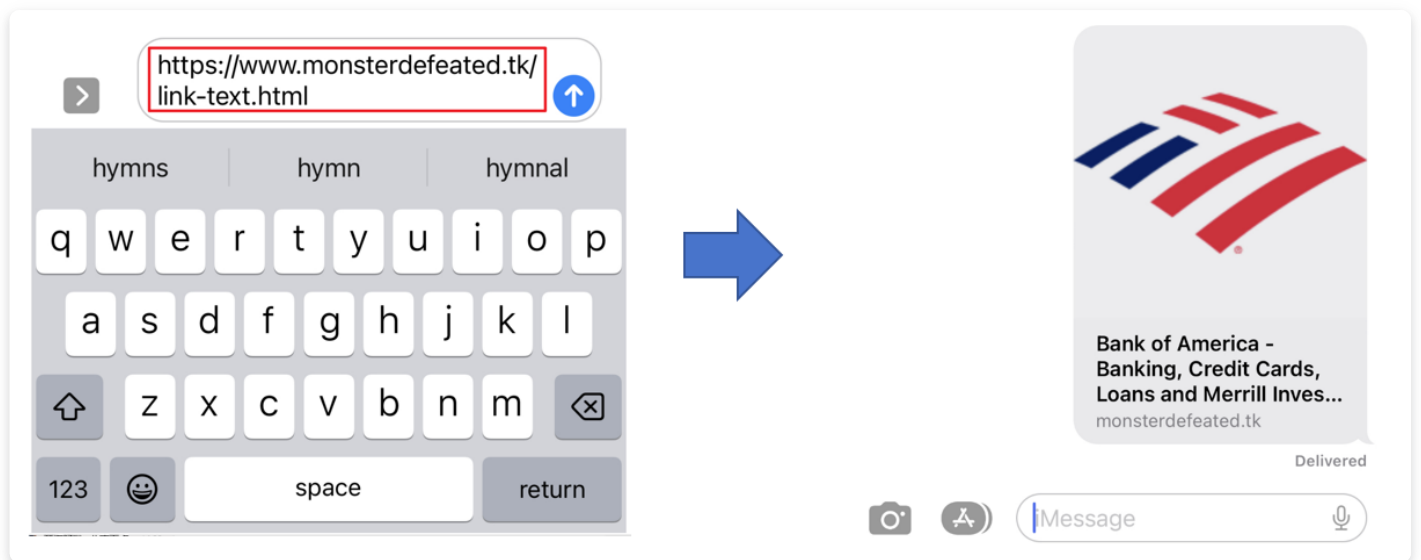


Figure 1: shared content preview based on OG protocol

However, this preview scheme can lead to phishing attacks. Since Apple's Messages app utilizes the OG (Open Graph) protocol for link previews, attackers can deceive the message receivers by disguising the phishing web pages using the OG protocol (shown in Figure 2).

In this way, the phishing page will be previewed as a harmless and trustworthy shared content as shown in Figure 1.

# Phishing page !!!

**BANK OF AMERICA** 

Checking

Savings & CDs

User ID

Password

☐ Save User ID

Log In

Forgot ID/Password?

Security & Help

Enroll

Open an Account

## Forge the OG protocol attributes

```
<meta property="og:title" content="Bank of America - Banking, Crec
<meta property="og:description" content="What would you like the p
ity. At Bank of America, our purpose is to help make financial liv
<meta property="og:type" content="website">
<meta property="og:image" content="./images/Bank-US.png">
<meta property="og:url" content="https://www.bankofamerica.com/">
<meta property="og:site_name" content="Bank of America">
```

Figure 2: forge the OG protocol attributes in the phishing page

## How to reproduce

We need a pre-made phishing page, and then we only need to add the following fields to the header of the page.

```
<head>
  <meta property="og:title" content="XXX" />
  <meta property="og:description" content="XXX" />
  <meta property="og:type" content="XXX" />
  <meta property="og:image" content="XXX" />
  <meta property="og:url" content="XXX" />
  <meta property="og:site_name" content="XXX" />
</head>
```