**Report on:**

### Capture location information of a device using a phishing link

#### SUBMITTED BY

**SUPRIYA SINHA (52)(SE)(ECS)**



**DEPARTMENT OF ELECTRONICS AND COMPUTER SCIENCE ENGINEERING**

**SHREE L. R. TIWARI COLLEGE OF ENGINEERING,**

**KANAKIA PARK, MIRA ROAD (E) – 401 107**

**UNIVERSITY OF MUMBAI**

**Academic Year 2022–2023**

### INDEX

#### ABSTRACT

1. PROBLEM STATEMENT

#### INTRODUCTION

1. Working

#### Expected Output

1. CONCLUSION
2. REFERENCE

### ABSTRACT

## URL Phishing - A Malicious Website

[Phishing attacks](https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/) commonly begin with an email and can be used in various attacks. URL phishing attacks take phishing a step further to create a malicious website. The link to the site is embedded within a phishing email, and the attacker uses social engineering to try to trick the user into clicking on the link and visiting the malicious site.

## How Does It Work?

URL phishing attacks can use various means to trick a user into clicking on the malicious link. For example, a phishing email may claim to be from a legitimate company asking the user to reset their password due to a potential security incident. Alternatively, the malicious email that the user needs to verify their identity for some reason by clicking on the malicious link.

Once the link has been clicked, the user is directed to the malicious phishing page. This page may be designed to harvest a user’s credentials or other sensitive information under the guise of updating a password or verifying a user’s identity. Alternatively, the site may serve a “software update” for the user to download and execute that is actually malware.

## 

## How to Identify URL Phishing

URL phishing attacks use trickery to convince the target that they are legitimate. Some of the ways to detect a URL phishing attack is to:

* **Ignore Display Names:** [Phishing emails](https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/phishing-email/) can be configured to show anything in the display name. Instead of looking at the display name, check the sender’s email address to verify that it comes from a trusted source.
* **Verify the Domain:** Phishers will commonly use domains with minor misspellings or that seem plausible. For example, company.com may be replaced with cormpany.com or an email may be from company-service.com. Look for these misspellings, they are a good indicators.
* **Check the Links:** URL phishing attacks are designed to trick recipients into clicking on a malicious link. Hover over the links within an email and see if they actually go where they claim. Enter suspicious links into a phishing verification tool like phishtank.com, which will tell you if they are known phishing links. If possible, don’t click on a link at all; visit the company’s site directly and navigate to the indicated page.

**INTRODUCTION**

IP address

An Internet Protocol address is a numerical label such as 192.0.2.1 that is connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions:

1)Network interface identification

2)Location addressing.

## **IP logger**

## An IP logger is a link that helps collect information about any device, or you can gather any information by tracking IP addresses. Internet protocol is very important to use an IP logger to track location. To hide the IP logger, you can use a VPN. Trojan: Win32/Hynamer.C!ml Iplogger.org site can be automatically launched based on the final result.

## 

### PROBLEM STATEMENT

### Capture location information of a device using a phishing link

### WORKING

### The project is determined to create a Capture location information of a device using a phishing link.

### Where is the person you’re talking to located? Are they who they say they are? To check, you can have that person click a special link. You’ll see their IP address, and that will tell you their rough location.

## How IP Tracking Links Work

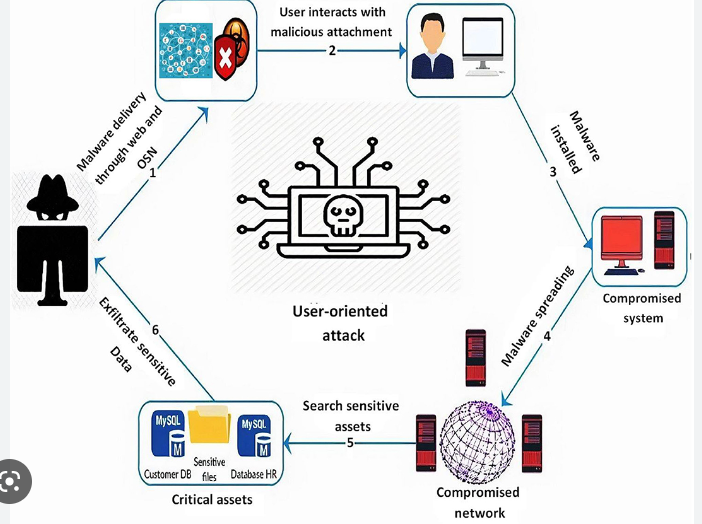
when someone accesses a resource online, the server sees their unique IP address. And IP addresses are tied to rough geographic areas. But popular web services don’t usually show you the IP address of that person, although you could certainly see it yourself if you were hosting your own web server. The method here uses an online service that “wraps” a real link for you, tracking the IP address that accesses it before quickly sending the person to the real target of the link.

This has its limitations. Anyone can use a [VPN](https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/) to mask their real location. But, even if they are, there’s a good chance the VPN will show a different location from where they claim to be. In the case of our fake job recruiter, the scammer claimed to be in the US, but they accessed our link from an IP address based in Nigeria.

If you don’t already know the location someone claims to be from and are just trying to figure out whether they’re genuine, you’ll need to convince the person to say where they are before sending them the link.

Once you do, you’ll need to prepare a digital file to send them. A picture, a Word document, or anything you can attach to a cloud storage link will do. If you’re dealing with a possible scammer, that scammer might ask you to send them something as part of a scam. If you’re dating online, you might want to send a photo. Once you’re ready to send a file, you’ll need to wrap that normal link with an IP tracking service.

Unfortunately, that process creates a link that’s obviously for tracking. You’ll need to use another service to hide that. You probably don’t want the other person to spot your trick.

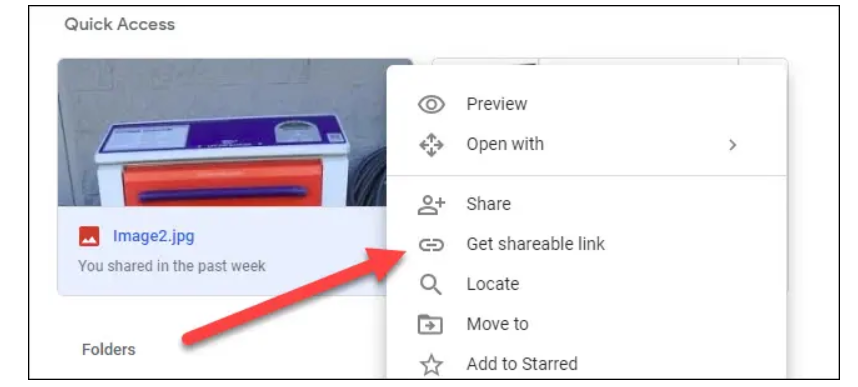


## How to Create a Disguised Tracking Link

You can use a link to any web page online, but this process will guide you through creating a link that goes to one of your files or photos.

The first step is to upload your file to a cloud service like Dropbox or Google Drive. If you suspect the person you’re interacting with isn’t trustworthy and you don’t want to give any personal information away, it’s a good idea not to use any main account you have. You may want to create a second “throwaway” account if you don’t already have one.

With your file uploaded, use the website to create a shareable link. In Google Drive, you can right-click on the file and choose “shareable link.” In Dropbox, hover your mouse over the file and select share.



This is the link your suspected scammer will land on at the end of the process. But don’t give this link to them. By itself, it tells us nothing.

Instead, go to the [IP logger website](https://iplogger.org/) and paste your URL into the “URL and Image Shortener” field. Click the “Get IPlogger code” button below it.



## 

The next screen will give you an “IP logger link for collecting statistics” and “link for viewing statistics.” Copy the “viewing statistics” link to a safe spot. This is what you’ll use to see the person’s IP address and location afterward.

The link for “collecting statistics” is the one with IP tracking in it. Unfortunately, that “iplogger.com” link will be a dead giveaway to your recipient.

## 

## 

To hide what you’re doing,  you can use a URL shortening service. Unfortunately, those shortening services don’t like the IP Loggers URLs and generate errors. To get around this, click on the iplogger.org drop-down to the right of “Select a domain name” and choose “2no.co” for your domain. The tracking link at the top will update, copy that new link.



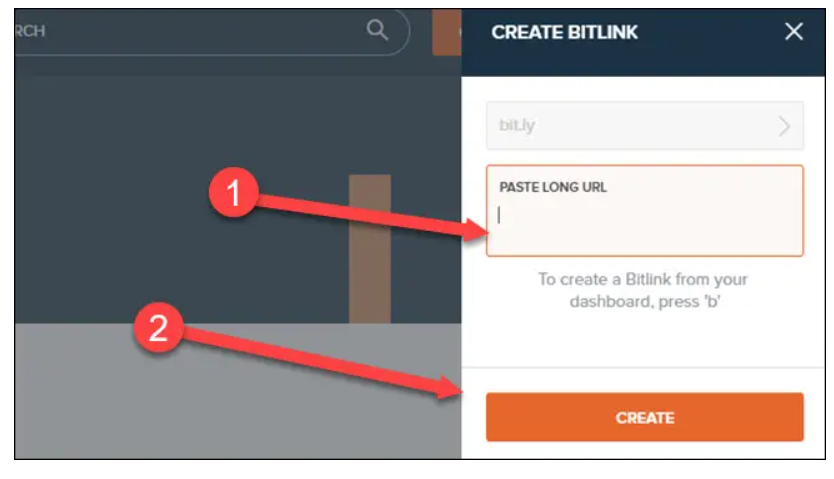
## 

Next, go to [bit.ly](https://bitly.com/)—you can try another shortening service if you prefer, but we tested with Bitly. If you don’t already have an account, create one.

Click the “Create” button in the upper right-hand corner of the Bitly website.

## 

Paste your 2no.co tracking link into the “Paste long URL” box and click the “Create” button.



## 

You now have a Bitly link you can give to your potential scammer. You can click the copy button to retrieve it quickly.

## 

## How to See the Recipient’s IP Address

Send that link to the person you’re talking to as you would a standard link. After you have, go back to IP logger, copy the viewing statistics link, and paste it into your browser.

You’ll see a list of any IP addresses that accessed the link, what location they’re from, and possibly what browser they’re using.

 Remember, this won’t tell you everything. If the person is using a VPN or similar technology, you won’t see their true location. But it’s one more tool in your arsenal to spot people who aren’t who they claim to be. If your tracking results show a different country than you’re expecting, be wary and consider walking away.

## How to Prevent and Protect Against Phishing

To help prevent phishing attacks, you should observe general best practices, similar to those you might undertake to avoid viruses and other [malware](https://www.comptia.org/content/articles/what-is-malware).

First, make sure your systems are updated to help protect against known vulnerabilities. Protect devices and systems with reputable security software and firewall protection. You can also add software that watches for PII being sent over email or other insecure methods.

Since the weak link in phishing attacks is the end user, you should provide proper [end-user security awareness training](https://www.comptia.org/content/videos/cybersecurity-awareness-training) and educate your team on how to recognize a phishing scam. The key to protecting against phishing lies in the ability to recognize the cyberattack as illegitimate. Following are some key concepts to include in end-user training:

* Instruct users to choose [strong passwords](https://www.comptia.org/blog/security-awareness-training-passwords) and be wary of posting your personal details on social media. Information like birthdates, addresses and phone numbers are valuable to an attacker.
* If there are any suspicions about an email or social post, contact the IT team to have them examine the situation.
* Only open attachments from a trusted source. When in doubt, check with the alleged sender directly.
* Note any language differences in messaging or emails that vary from legitimate organizational communications.
* Never give away personal information in an email or unsolicited call. For instance, financial institutions will never call and ask for login credentials or account info because they already have it.
* Inspect emails for typos and inaccurate grammar. This is usually a dead giveaway of less-sophisticated phishing scams.
* Don’t supply personal information via email or text.
* Beware of urgent or time-sensitive warnings. Phishing attacks often prompt action by pretending to be urgent.
* Verify emails and other correspondence by contacting the organization directly. If you think something is fishy (okay, bad pun), a phone call can quickly identify a legitimate call from a fake one.

Conclusion

Phishing campaigns can be difficult spot. Cyber criminals have become experts at using sophisticated techniques to trick victims into sharing personal or financial information.

But the best way to protect yourself is to learn how to spot a phishing scam before you take the bait.

### LITERATURE SURVEY

1. <https://www.getcybersafe.gc.ca/en/blogs/phishing-introduction>
2. <https://iplogger.org/>
3. <https://www.howtogeek.com/410897/how-to-track-someones-ip-and-location-with-a-link/>
4. <https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full>
5. <https://medium.com/@hamzamujeebk/how-to-track-someones-location-by-sending-them-over-a-link-74324c658735>
6. <https://www.ehacking.net/2022/01/how-to-track-phone-location-by-sending-a-link-track-iphone-android.html>
7. <https://warrenaverett.com/insights/what-happens-if-you-click-on-a-phishing-link/>