What is IPFS Phishing attack? How to avoid?

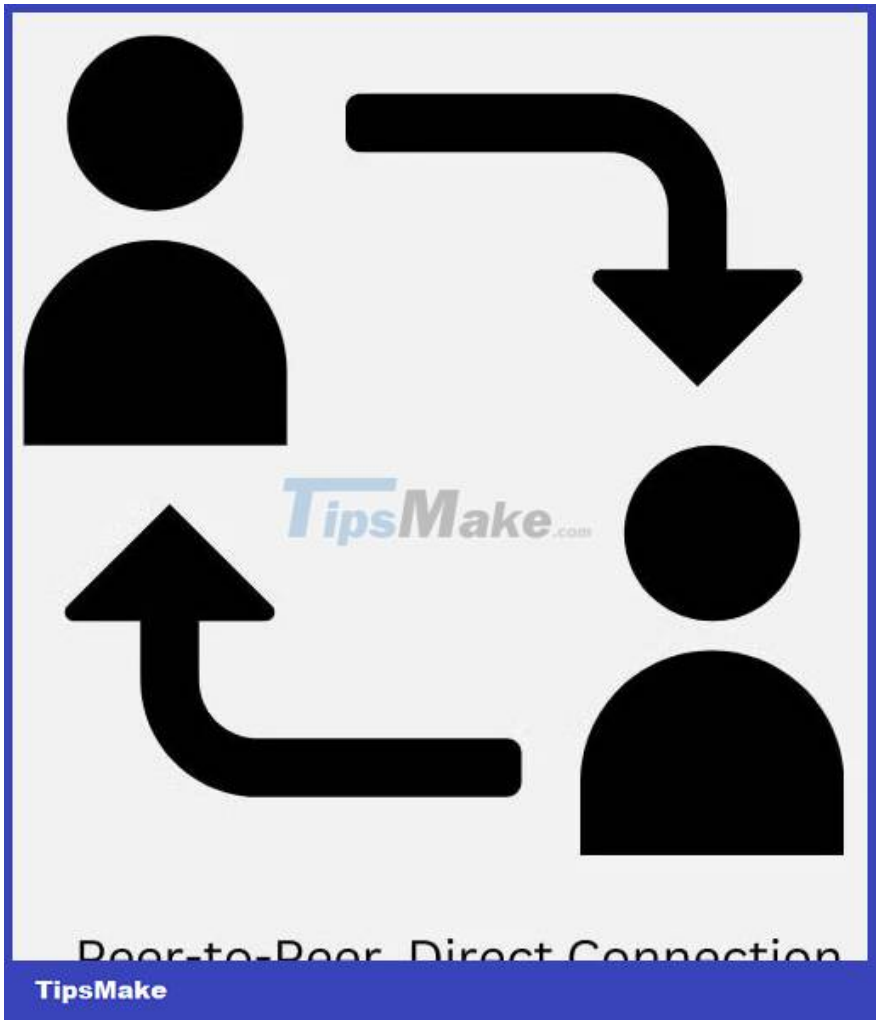
While the InterPlanetary File System (IPFS) offers many benefits, it also allows cybercriminals to carry out malicious campaigns.

Phishing techniques have continued to evolve, especially with the advent of new, advanced technologies. While the InterPlanetary File System (IPFS) offers many benefits, it also allows cybercriminals to carry out malicious campaigns.

These attacks become even more dangerous as many file hosting, web hosting and cloud services now use IPFS. So what are IPFS Phishing attacks and how can you prevent them?

What is IPFS Phishing attack?

IPFS replaces Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) as a way to deliver the World Wide Web. Unlike its location-based predecessors, IPFS is a distributed file system. Instead of the traditional centralized client-server approach, IPFS uses a peer-to-peer (P2P) data network located around the world without requiring a third party or centralized authority.



Due to the decentralized nature of IPFS, malicious actors are increasingly using P2P data sites to trick gullible individuals into revealing sensitive information or installing malware. These criminals take advantage of the IPFS network to host their Phishing toolkit infrastructure, as they can easily disguise their activities.

Additionally, any malicious data uploaded to one of the connected networks (or nodes) can be distributed to other nodes. In addition, these malicious files can only be deleted by their owners.

As a result, IPFS Phishing content can be easily distributed, difficult to detect, and persistent.

Types of Attacks IPFS Phishing

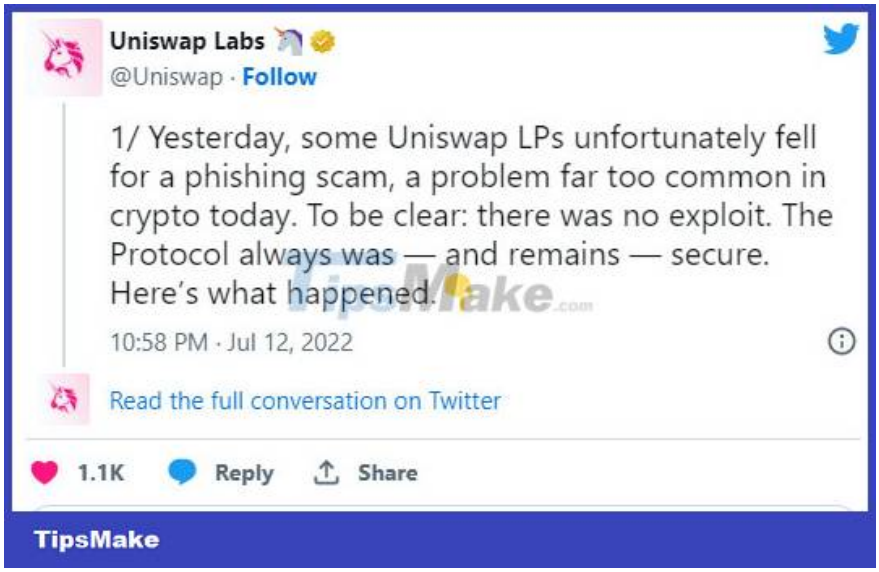
IPFS Phishing attacks can target specific individuals instead of some random users. However, mass IPFS Phishing campaigns are more common.

To facilitate attacks, these malicious actors use one of the following methods:

1. **Malicious URLs** : Attackers use text messages, emails, direct messages (DMs), pop-ups, or other channels to trick you into clicking a link that leads to a malicious IPFS gateway.
2. **Spoofing Domain Name System (DNS)** : In addition, these malicious actors can create a fake DNS server that will redirect you to a malicious IPFS gateway hosting a fake website.
3. **Fake Secure Sockets Layer (SSL) Certificates** : Also, they can use fake SSL certificates to convince you that you are visiting a legitimate website.

Examples of IPFS Phishing attacks

In July 2022, attackers distributed a fake token disguised as a Uniswap (UNI) token to more than 70,000 wallet addresses of liquidity provider Uniswap (LP). These hackers embedded code into the malicious token's smart contract, allowing their fake website to carry the Uniswap brand.



How do IPFS Phishing attacks work?

IPFS Phishing attackers take advantage of reputable websites, apps or data to fool gullible people.

First, they create a fake website or app that looks like the legitimate version. They then host this rogue platform on the IPFS network.

Although IPFS is primarily available over a P2P network, some public IPFS gateways - such as ipfs.io or dweb.link - allow traditional web users to access IPFS. These scammers use these ports as proxies, so you can access files on the IPFS network even if you're not running the IPFS client.

After creating fake websites and hosting them on gateways, Phishing attackers will lure you into accessing their fake gateways. They can send you mail, text messages, DMs, or text you in an app, such as a game or productivity app.

For example, a Phishing attacker sends you a PDF file that is believed to be related to DocuSign, the document signing service. After clicking the **"Review Document"** button , it looks like you're on a Microsoft authentication page, as it's actually a fake website hosted on IPFS. If you insert your email address or password, the attacker will collect your details and potentially use them for further attacks.

These attackers can use any subject line or file format as long as they can get you to click their malicious link.

3 common signs of IPFS Phishing attacks

To avoid IPFS Phishing attacks, you must recognize how they appear. Here are 3 common signs of these malicious attacks:

1. Unsolicited Messages or Direct Messages

Phishing attackers primarily send text messages, emails, or direct messages prompting you to click on a link, often unexpectedly. They may ask you to pay taxes, authenticate, update your account, or other similar requests and orders that appear to be unwarranted.

These messages are generally general and may not specifically address you. Sometimes, IPFS Phishing attackers ask you to act quickly so as not to lose something or get in trouble.

In addition, these scammers sometimes act as legitimate platforms. They will send unexpected instructions asking you to do something. But most companies will never ask for sensitive customer details via email, text or

direct message.

2. Suspicious URL or SSL certificate

While it's best to avoid clicking on links in emails, texts, or direct messages, if you click, you may notice that the URLs don't match the URL of a legitimate website. The website's SSL certificate may also be invalid or different from the original website's certificate.

3. Malicious IPFS gateway

If you notice 'IPFS' or 'CID' in a link and the website you are trying to visit is not hosted on IPFS, it could be a sign of a Phishing attack. These identifiers can be at the beginning or end of the URL.

Pages hosted on IPFS have URLs that look like this: *'https:///ipfs/'* , where CID is the resource's content identifier. Instead of CID, you can look for IPNS ID or DNSLINK, which are also links to resources. Instead of links to this resource, you can also find a random string of 46 characters.

However, if you are on an IPFS network, you can check the gateway used in the URL to determine if the gateway is malicious or secure.

10 tips to stay safe with IPFS

You need to adjust your defenses to keep up with the evolution of Phishing attacks. Apply the following tips to avoid IPFS Phishing attacks.

1. Keep your browser and software up to date with the latest security patches.
2. Try to insert the URLs manually or use bookmarked links. If not, double-check the links to make sure they're legitimate sites.
3. Use two-factor authentication (2FA) whenever possible to protect your account from unauthorized access.
4. Make sure you only use trusted IPFS gateways. Stay away from unknown gateways.
5. Protect your device with up-to-date antivirus products.
6. Always verify instructions in emails, text messages, or direct messages through official communication channels, especially if they are random or unexpected.
7. Check any IPFS gateway SSL certificates. Alternatively, you can install IPFS Companion to securely interact with the network through your browser.
8. When using the IPFS gateway, you can use a virtual private network (VPN) to hide your private address. Note that VPN will not work if you run an IPFS node.
9. Use web filters to block IPFS-based phishing sites.
10. Stay up to date with IPFS trends, as cybercriminals will likely find more sophisticated techniques to support their malicious programs.

The bad guys are constantly finding new ways to carry out Phishing attacks. They have already started using the IPFS network to do this.

However, anti-spam methods and many other solutions can limit these attack attempts. So be aware of the latest technological advancements and cyber threats to stay safe.

You finished reading the article "**What is IPFS Phishing attack? How to avoid?**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.