



## **What Is Phishing ?**

Phishing is a form of social engineering in which hackers trick people into revealing personal information or installing malware such as ransomware. The hacker creates a fake website based on the target's interests and sends the website link to the target via email or other similar means. As of 2020, it is the most-reported cybercrime, with the FBI's Internet Crime Complaint Center reporting more phishing incidents than any other type of computer crime.

The term "phishing" was first recorded in 1995 in the cracking toolkit AOHell, but may have been used earlier in Hacker Magazine in the 2600s. This is a variation of fishing and refers to appealing to "fish" for sensitive information.

## **Some example of Phishing :-**

### **Email Phishing**

Phishing attacks, often delivered via email spam, attempt to trick individuals into providing personal information or login information. Most attacks are "bulk attacks" (untargeted). They are sent to everyone at random. Hackers' targets can vary, with common targets including financial institutions, email and cloud productivity providers, and streaming services.

Stolen information and access may be used to steal money, install malware, or phish others in the target organization. Stolen streaming service accounts may also be sold on darknet markets.

### **Spear Phishing**

A targeted phishing attack that uses personalized emails to trick a specific person or organization into believing they are legitimate. Original personal information is used to increase the chance of success. These attacks often target executives or people in finance departments who have access to

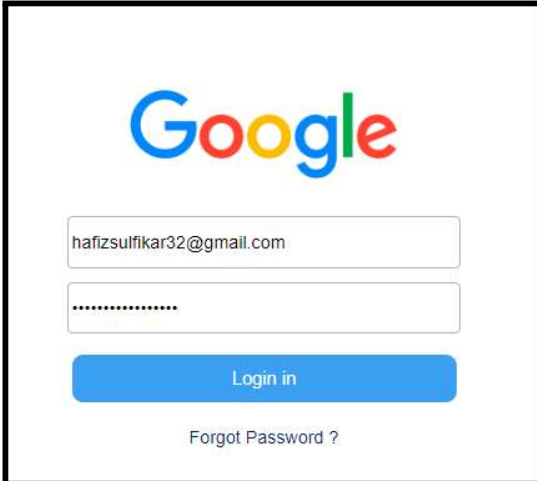
sensitive financial data and services. Accountancy and audit firms are particularly vulnerable to phishing due to the value of the information their employees have access to.

Threat group-4127 Fancy Bear (Russian espionage group) targeted Hillary Clinton's campaign (former US Secretary of State) by using the accounts-google.com domain to spear-phishing more than 1,800 Google accounts.


A study of spear phishing susceptibility among different age groups found that 43% of 100 young adults and 58 older adults clicked on simulated phishing links in daily emails over a 21-day period. Whaling and CEO Fraud  
Whale attacks use spear phishing techniques to target senior executives and other high-profile individuals[23] with customized content, often related to a subpoena or customer complaint.

CEO fraud involves sending fake emails from senior executives to trick employees into sending money to an offshore account.[25] This has a low success rate but can result in huge losses for firms.

### Operation of Phishing Website



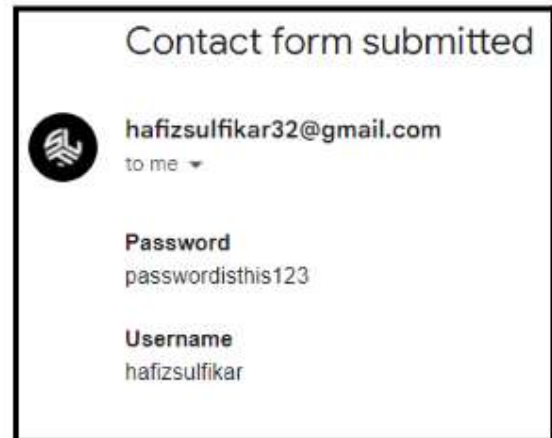
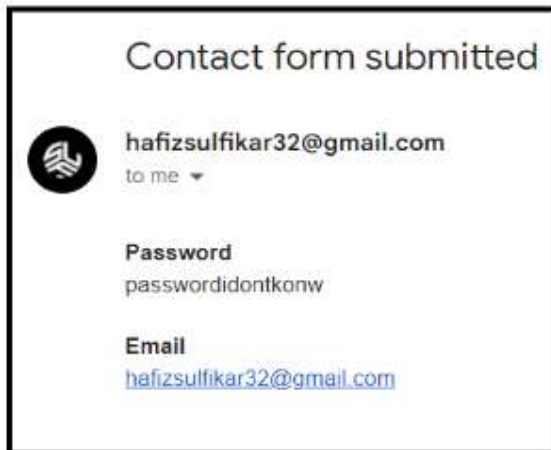
A screenshot of a phishing website designed to look like Google's login page. It features the Google logo at the top. Below it is a text input field containing the email address 'hafizsulfikar32@gmail.com'. Underneath the email field is a password input field with masked characters (dots). At the bottom of the form is a blue 'Login in' button. Below the button is a link that says 'Forgot Password ?'.



A screenshot of a phishing website designed to look like Instagram's login page. It features the Instagram logo at the top. Below it is a text input field containing the username 'hafizsulfikar'. Underneath the username field is a password input field with masked characters (dots). At the bottom of the form is a blue 'Login in' button. Below the button is a link that says 'Forgot Password ?'.

Hacker's login details are obtained by clicking the login button after typing in details like email and password.

**Like this ↓**



## How to recognize a phishing website?

### **1. Check the URL**

To learn how to identify phishing URLs, you need to verify the authenticity of the web address. If it starts with 'http://' instead of 'https://', be careful. The extra 'S' means the website is encrypted and secured with an SSL certificate. An SSL certificate is like a code that promotes additional security for online communications. However, nowadays, phishers are also starting to use 'https://', so this aspect is not a foolproof sign.

### **Take a closer look at some other ways to check for phishing links:**

Usually, fake websites have an extra letter 'S' or 'A' in the spelling. For example, [www.walmarts.com](http://www.walmarts.com) or [www.flipkaart.com](http://www.flipkaart.com). If 'O' is replaced by '0' (Zero). For example, "[www.yah00.com](http://www.yah00.com)." If the URL has extra or missing characters or symbols. For example, a legitimate URL is [www.coca-cola.com](http://www.coca-cola.com) (with a hyphen), but a fake URL might be [www.cocacola.com](http://www.cocacola.com) (without the hyphen).

### **2. Compare content quality**

Original website content should be good, well written and free of grammar, punctuation and spelling errors. Although the fake site is a carbon copy of the original site, the visuals may be of lower resolution.

### **3. Check for missing content**

Do you know how to identify phishing URLs with one click? Go to the "Contact Us" page. If there are no reliable contact details, it could be a phishing website.

### **4. Requesting Personal Information?**

If a pop-up appears asking for personal details like your phone number, email address, password, residential address, banking details, ID number, etc., consider this a red flag. In this case, always refrain from providing any kind of information. You can share this advice with acquaintances, work colleagues and employees who want to know how to identify a phishing website.

### **5. Is this an unsafe website?**

Sometimes, you try to visit a website, but you get a security alert—'Connection Not Secured.' In such a situation, it is very important to understand how to identify phishing links. First, click on the padlock icon that appears to the left of the URL. In this way, you can avail yourself of information related to security certificates and cookies. A cookie is a file that stores a user's data and sends it to the website owner. In most cases, this provides a better user experience; However, phishers often misuse this information.

### **6. Use a fake password**

If a suspicious website asks for a password, enter an incorrect one. If you are still signed in or see the point indicating that you entered the correct password, it is 100% fake website. This trick will help you avoid these social engineering attacks.

### **7. Check the payment method**

If a website asks for a direct bank transfer instead of debit cards, credit cards, and payment options like PayPal, you need to be cautious. This may indicate that no bank has approved credit card facility for the website domain and they may be practicing malicious activities. Especially when spending large sums on software-based services where delivery is not fast, check out a Request for Proposal.

## **How to report a phishing website**

Now that you have a reasonable understanding of how to know if a link is a phishing URL, you should also learn a simple way to report a phishing website. The global pandemic, series of lockdowns and rising unemployment have increased the number of fraudsters. Google reports an average of 46,000 new phishing websites every week in 2020.

If you see such suspicious websites, go to Google's report phishing page. Add more information by providing a URL.

[https://safebrowsing.google.com/safebrowsing/report\\_phish/?rd=1&hl=en](https://safebrowsing.google.com/safebrowsing/report_phish/?rd=1&hl=en)

**© CYBER SLF | DIRECTOR: HAFIZ SULFIKAR**