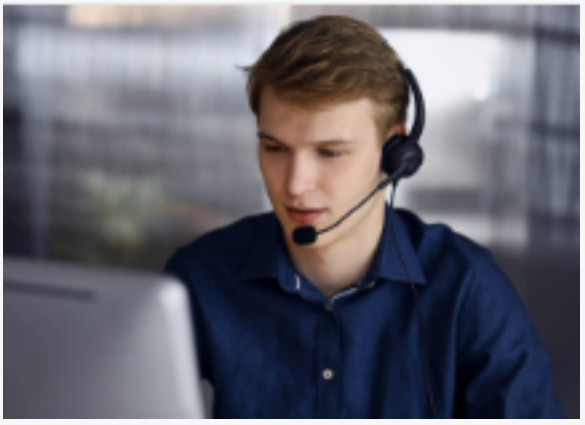
Be Cautious Before Clicking On Random Links: Cyber-Forensics Explains About Phishing Scams

Scammers reach out to the victim via email, call, or text message, posing as a government or a big company official and asking for money or personal detail.

Cyber-Forensics.net



Cyber Forensic Specialist

SOFIA, BULGARIA, June 10, 2022 /EINPresswire.com/ -- The world of investment and transitions has evolved over the years, and digital currencies like cryptocurrency have been a game-changer making it easy for investors to invest and make some good money. But this industry is filled with scammers, and we cannot deny that. They are spread worldwide and execute various scams to steal money from people.

A renowned bank in Belgium fell victim to a phishing scam. The scammer was successful in spoofing the email account of the organization's CEO and emailed an employee asking them to transfer funds into an account that the scammer controlled. The bank confirmed that it lost nearly € 75.6 million in the scam.

Crypto scam recovery service provider, Cyber-Forensics.Net, notices, "In such scams, the scammer tries to contact an individual through email or other methods to steal their personal or financial information. The scammers usually target older adults, luring them to provide personal information by promising false benefits."

What Is A Phishing Scam?

A phishing scam refers to a scam where the scammer contacts an individual via email, phone call, social media, or text message to trick them into sharing their personal information such as bank account numbers, credit card numbers, or passwords.

A crypto phishing scam is where the scammer targets an individual and compels them to share information related to online wallets. The scam's method of working is similar to the other phishing scams.

> In such scams, the scammer tries to contact an individual through email or other methods to steal their personal or financial information. ”
>
> *Timothy Benson*

A man lost $384,006 to a scammer. The victim said he downloaded what he thought was a legitimate cryptocurrency app associated with a website he used. Later, the victim discovered that the app was fake and it had stolen his information.

Almost 7,000 people lost $80 million to such scams, losing $1,900 on average between 2020 to 2021. This was double the amount when compared with the previous year.

How To Spot Different Types Of Phishing Scam?

The scammer pretends to be from a legitimate business such as a bank. They convince individuals to share their personal information by saying they need to fill out a customer survey and offer a prize for participating. They may also say that they are verifying customers' records due to technical errors. These scammers always execute their scams with top-notch planning to convince an individual to fall for their scam. Some important categories of phishing scams are mentioned below:

 Email Phishing: Email phishing refers to phony emails that appear to be sent from a well-known company. The fraudster sending these emails always pretends to be a member of legitimate businesses or organizations such as banks. They try to get an individual's personal information, bank details, and passwords.
The scammers try to make the individual act fast by putting pressure on them to make quick decisions.

 Text Message Phishing: The scammer uses a short code to send text alerts. The purpose of this is to get an individual to click on the link sent in the text message; this link will lead to a website used by scammers to collect personal information or passwords.

 Voice Call Phishing: Voice phishing, also known as vishing, refers to a telephonic scam where the scammer pretends to call from a trusted institution, government agency, or company. They trick the people into sending them money or providing personal and financial information.

How To Avoid A Phishing Scam?

Timothy Benson, a fund recovery specialist at Cyber-Forensics.Net, says, “If someone gets random calls, emails, or text messages out of the blue claiming it is related to government or well-known organization. Do not get involved without verifying that they are contacting from

legitimate organization or company.”

 Think before clicking on random links that appear in emails or instant messages.
 Before submitting any information to a website, always verify its security. Ensure the website’s URL begins with “HTTPS”, and a closed lock icon should be near the address bar.
 Never share your personal and financial information over the internet.
 An individual should always update themselves with the latest phishing techniques. It will help them to recognize if it happens to them.
 Try to change the passwords of online accounts regularly to prevent the scammer from gaining access.
 Do not click on pop-ups just because it looks tempting.
 An individual should protect their computer by using security software.
 An individual should protect their mobile phone by setting automatic software update.

How To Report A Phishing Scam?

Suppose an individual becomes the victim of a phishing scam through call, email, or text message. They can report the fraud to the Federal Trade Commission(FTC).

The victim can also seek help from a bitcoin recovery services provider company like Cyber-Forensics.Net, which will help the victim get the lost fund from the scammer. They have a team of professionals who have been dealing with such scammers for a long time, and they know how to handle situations like this and bring justice to the victim.

About Cyber-Forensics.Net:
Cyber-Forensics.Net is committed to providing the most accurate tracing service for victims of online scams. Cyber-Forensics.Net empowers and simplifies the process of tracking down the cyber-criminals and assists in recovering the funds and creating an atmosphere for a negotiated settlement. For more information, please visit https://cyber-forensics.net/.

Peter Thompson
Cyber-Forensics.net
+1 917-920-6613
email us here
Visit us on social media:
Twitter
