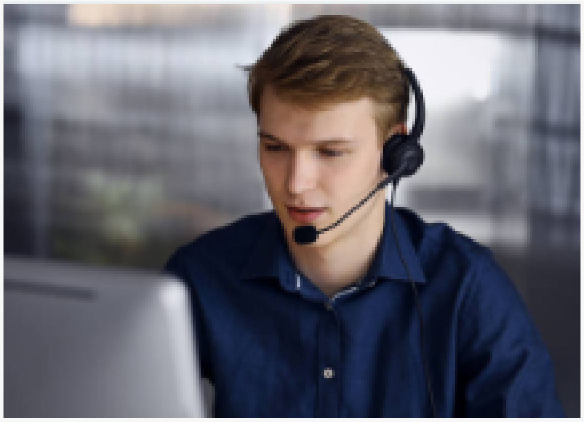
EINPRESSWIRE

Phishing scam becoming more sophisticated: Cyber-Forensics.net experts suggest prevention tips

Cyber experts suggest phishing scams rising amid the pandemic. Scammers using compromised links are stealing information from unsuspecting customers.

SOFIA, BULGARIA, December 8, 2021 /EINPresswire.com/ -- Phishing scam becoming more sophisticated: Cyber-Forensics.net experts suggest prevention tips

Cyber-Forensics.net


Cyber Forensic Specialist

Cyber experts have spotted various types of phishing scams rising amid the pandemic. Scammers are sending emails with compromised links to steal information from unsuspecting customers.

Significant research by leading organizations highlight emerging trends in the phishing scam. The reports revealed fraudsters impersonating email domains of the top government organizations and tricking people into giving valuable information.

Platforms like Cyber-Forenics.net are stepping forward with protective measures to halt the increasing numbers and create awareness among users.

> “The more use of the internet and focus on digitalization has resulted in rising phishing attacks.”
>
> *Chief analyst at Cyber-Forensic.net*

A part of the effort observed Cyber-Forensics.net, a leading expert in cyber forensic services for online scam victims, to lay down the common phishing scams that baffled millions across the globe.

Speaking about the rising cases, a chief analyst at Cyber-Forensic.net explains that “the more use of the internet and focus on digitalization has resulted in rising phishing attacks. With more and more individuals choosing to work online, they forget basic security steps that can prevent malicious attacks."

Covid-19 Scam

How do Phishing scams work?
In phishing scams, attackers send compromised links through email. When the users click that link, they are directed to fake websites which promise rich rewards, medical treatments, and many other baits. However, these websites ask the users to provide personal information first to claim their prizes, reward points, etc.

According to reports, in the first half of November 2021, around 44.9 million people fell victim to covid-19 variant Omicron related phishing scams. Investigations revealed that scammers sent emails with compromised links.

The fraudsters impersonated government websites and asked for personal information such as bank details, names, date of birth, email address. Once the user clicked the links, their bank details were stolen.

How to identify a phishing scam?
The best way to escape becoming a victim of any phishing scam is to be aware of certain patterns that tricksters use to trap innocent people. In many cases, identifying the signs may be difficult even because cybercriminals are astonishingly convincing. Still, some ways can help you know if it is a scammer or a legitimate organization.

Check the source of the message: Always check the origin of the message sent. If the message appears to be sent via an unknown source or email address, chances are it is a scammer. Trusted agencies have their official email addresses and phone numbers available on the website.

Check URLs of the website before clicking: An authentic webpage usually starts with the https://www header. If the click in the message doesn't start with this header, it is possibly a phishing scam.

Check website logos: Scammers may replicate website logos, but to avoid legal implications, they usually alter or make a few changes in the symbols of the reputed organizations.

Check the email source: A good way to identify if the email is genuine is to look at the email header.

Look for Grammatical errors: Carefully check for each spelling, symbol, and grammatical error. And if any suspicions arise, the matter should be immediately reported

Ways to avoid becoming victims of phishing scams
According to cyber expert Timothy Benson, the best way to stay protected from phishing scams is to practice the following principles:

Never share personal information online: Experts say that individuals should never share their private information with an unsolicited request. This applied to all messages, emails coming from any suspicious or unknown source.

Report the suspicious emails: To validate whether the email is genuine or not? Contact the organization or institution through public channels through provided phone numbers and emails.

Resist the pressure to act immediately: Scammers push emotional responses by making their emails sound urgent. However, genuine organizations always give you time to decide.

Sign for a free scam alert: Stay updated with rising phishing scams on the news and gather the details of the latest scams and essential advice from Federal organizations or agencies that deal in cybercrimes such as Cyber-Forensics.net

Never share passwords/ OTP: Be aware that official sources never ask for a password to validate one's identity. Only scammers and cybercriminals ask for such pins and passwords.

Keep checking account activity from time to time: It is better to maintain account passwords regularly.

The tips mentioned above are helpful in keeping the accounts safe. But in case an account has already been hacked and scammed individuals into losing money, there are legal procedures that should be followed to retrieve the lost amount. The first crucial step towards retrieving the money is by identifying the right online scam victim help services.

How to choose the right scam help expert?
A good start is by seeking expert advice from online scam help services. But the problem arises when scam victims do not know which services may provide accurate help. Cyber expert Timothy Benson says; What is worse than being scammed is not finding the right support by services claiming to be experts in their field."

He further adds by explaining that a great scam help service should consider all the pain points of the online scam victims. In phishing scams, the biggest problem that scam victims encounter is locating the scam's source or origin. Cyber experts help find the origin of the fraud and malicious links leading to a strong case that can work in favor of the victims.

Is hiring a cyber specialist beneficial for online scam victims?
As internet platforms become more accessible and easily penetrable, cyber specialists can help protect the integrity of businesses and individuals' data.

Cyber specialists work closely with renowned cyber security experts and legal practitioners to monitor, investigate, analyze, detect and respond to cyber security threats. With years of field experience and the right knowledge, they can help mitigate persistent and potentially catastrophic cyber threats.

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