

## Cyber-Forensics.net joins the Scam Awareness Week 2021 Campaign: Encourages consumers to speak up against covid-19 scams

More than 350 partners, including Cyber-Forensics.net across the United States, joined the fight this year under the theme "let's talk scams."

SOFIA, BULGARIA, November 9, 2021 /EINPresswire.com/ -- <u>Cyber-Forensics.net</u>, an industry leader in providing cyber-forensics services for victims of <u>online scams</u>, reported a parallel



outbreak of online scams in the covid-19 pandemic. As of 2021, the Federal Trade Commission reported approximately 625,000 consumer complaints related to Covid-19.

Statistically, newly released data by the FTC indicates that these scams have cost consumers an approximate \$587.2 million loss.



the more we talk about scams, the more awareness we have, and the harder it is for scammers to steal money or personal information."

Timothy Benson, Chief Analyst

However, as nations observe Scam Awareness Week 2021, world leaders feel compelled to address the issue immediately.

Understanding the urgency of the matter, reputed organizations are hopping on the Scam Awareness Week campaigns under the theme "Let's talk scams." It is an effort to initiate honest discussions aimed at helping

people detect and prevent falling victims to online fraud.

The U.S. Department of Health and Human Service Office of Inspector General stepped in to alert the public related to novel Coronavirus. Today, scammers use more and more sophisticated tricks like telemarketing calls, social media platforms, text messages, door-to-door visits, third-party payment apps to steal money and personal information from individuals.

To curb the same, the campaign welcomed more than 350 partners across all public and private platforms, including Cyber-Forensics.net joining the fight against online scams. The organizations say: "the more we talk about scams, the more awareness we have, and the harder

it is for scammers to steal money or personal information."

Cyber-Forensics.net chose to focus its campaign on covid-related scams, as scammers use coronavirus pandemic benefits to harm potential beneficiaries.

Leading the campaign, Cyber-Forensics.net urged consumers to speak up against scams alongside highlighting some of the precautions consumers can take to be aware of global security challenges.

For instance, with more organizations expecting what tactics scammers use, network safety can be strengthened beforehand.

What does Cyber-Forensics.net say to Protect Yourself from Covid-19 related scams?

Stay away from online proposals for Covid cure or quicker admittance to vaccination. They aren't authentic.

Be careful about messages, calls, and web-based media posts promoting "free" or government-requested COVID-19 tests. Look at the FDA site for a complete list of supported tests and testing organizations.

Try not to tap on the "join now" buttons in emails or download any link from an unrequited source, regardless of whether the email address seems as though it is an organization or individual. The same goes for short messages and new websites.

Try not to share personal data, for example, Social Security number, credit card, visa, Medicare, and Mastercard details, because of a spontaneous call, text, or email.

Stay away from sending money to "accidental money deposit emails" or calls or messages for COVID-19 victims, particularly if someone pressurizes you to make payments quickly and demands installments of any kind.

The Consumer Sentinel Network maintained by the Federal Trade Commission identifies 5 types of identity theft used by scammers: Government benefit applied for/received, credit card fraud, miscellaneous identity theft, business/personal loan, and tax fraud. Most of these take place through third-party payment applications.

These third-party app frauds are usually undetectable because most of them arise without anyone specific authority operating them. A fraudster combines different tactics like the accidental payment message, the withdrawal notice, and a friend in need to request payment and hack into the recipient's computer.

Another reason for the spike in cyberattacks is the way small to large organizations allow

individuals to use personal computers to access corporate records. Allowing employees to use personal computers doesn't ensure a similar degree of data protection as corporate-bought tools.

For instance, an organization's staff working on personal computers may not have a strong antivirus or malware installed. Additionally, home-enabled Wi-Fi networks are a lot simpler to pierce through.

If consumers don't realize these threats, cybercriminals may continue to steal their money. Strengthened cybersecurity protects all categories of data from theft and damage by investigating fraud and developing cutting-edge strategies.

## About Cyber-Forensics.net

Founded in 2021 and headquartered in Sofia, Bulgaria, 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/or creating an atmosphere for a negotiated settlement. For more information, please visit <a href="https://cyber-forensics.net">https://cyber-forensics.net</a>.

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

This press release can be viewed online at: https://www.einpresswire.com/article/555896607

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2021 IPD Group, Inc. All Right Reserved.