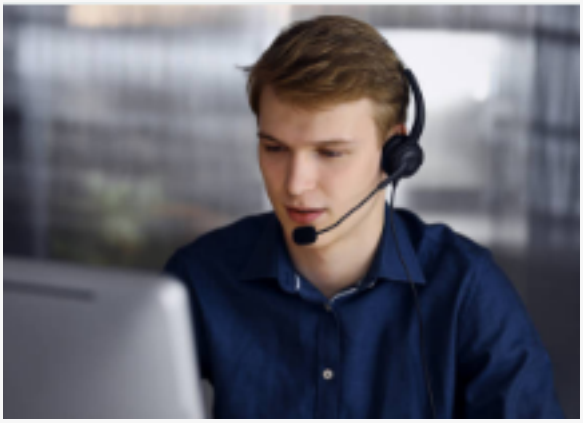
Buyers lose billions to online shopping scams: Cyber-Forensics.net explains payment fraud prevention techniques

Scammers are pretending to be legitimate online retailers, building fake websites and ads to steal banking and personal information from shoppers.

SOFIA, BULGARIA, April 14, 2022 /EINPresswire.com/ -- As businesses focus on frictionless customer interaction through online transaction facilities, online criminals are discovering new methods to defraud online shoppers. In a new technique to defraud online shoppers, scammers are pretending to be company representatives and stealing credit card information from buyers.

Cyber-Forensics.net



Cyber Forensic Specialist

According to a UK-based crime analysis firm, between 2020 and 2021, individual victims filed 448,838 reports, amounting to approximately 1.9 billion losses.

Cyber-Forensics.net, a cyber forensics service that has been actively using artificial intelligence-powered tools to assist online scam victims, reveals:

"Digital transactions may have changed our lives for the better. But, it has simultaneously opened up new avenues for criminals and perpetrators to exploit the loopholes in the systems. "

> The biggest problem with these online shopping frauds is the method of payment."
>
> *Timothy Benson*

How Do Online Shopping Scams work?

Scammers take advantage of the anonymous nature of the internet to target unsuspecting shoppers. They may even have access to the latest technology to set up their own fake websites and applications to execute various types of online scams.

Fraudsters make these websites appear real by using extremely sophisticated web design themes and layouts, including custom logos.

How to Catch Fake Online Shopping Scammers?

Timothy Benson, chief analyst at the firm, says, "many of these fraudsters even offer luxury items, including branded clothes, jewelry, and electronics, at lower prices."
But the catch with these types of scams is that instead of using the accurate domain name, scammers make some noticeable changes to their website's name, which, if shoppers are cautious, can be caught.
In most cases, online shoppers may even receive unsolicited text messages with fake discounts and offers. They ask for OTPs to run their scam and access the consumer's account that has all the credit card details.
Overall, tricksters will do everything in their power to get their hands on consumer details, Fund recovery service expert Peter Thompson states, "The biggest problem with these online shopping frauds is the method of payment."
Scammers often ask shoppers to complete their orders by paying the supposed bill amount using wire transfers that may be untraceable. However, experts warn that if customers pay using such methods, they may lose their sensitive information to scammers and never receive what they ordered.
But if shoppers are smart enough to recognize some warning signs, they can stay well protected.

Warning Signs of an Upcoming Online Shopping Scams:

Here are some of the warning signs to prevent falling victims to online shopping scams:

 Watch out if the product being advertised is unbelievably low-priced.
 Benefits from sales are understandable, but if the features sound too good to be true, it's a scam.
 The retailer insists on immediate payment using an unknown payment app. They may even insist that shoppers pay the billed amount to get access to cheap deals or give-aways.
 Their social media store doesn't offer store location details and offers very limited information about their products and services.
 The online retailer does not provide adequate information about their return policy, dispute resolution policy, shipping policy, or terms and conditions.
 The seller may claim they are overseas but may not provide exact details.
 The seller does not offer secure payment services for payment.

How to Stay Protected from Online Shopping Scams?

 Check official websites and social media accounts for popularity. Also, read about the return policy. Usually, credible brands offer a clear understanding of the handling process in case a

dispute arises.

 Learn about the site: When using online retail websites, make sure to do a background check and look for reviews.

 When making online payments, pay using secure payment services. Check the website for the "Secure" URL that starts with "https" and has an SSL certificate. Make sure to double-check the billed amount to be paid.

 Avoid any arrangement requested by retailers to pay order payment in person or anything that involves cash handling in the case of international orders. Scammers may create fake scenarios to somehow get victims to meet in person.

What to do if Targeted by Online Shopping scammers?

 Report the matter: If shoppers miss noticing the above warning signs and fall victim to the scammers' extremely sophisticated tactics, they should immediately report it to the local law enforcement.

 Secure credit card: Block the credit card immediately and notify the bank. They will be able to make sure unauthorized transactions are frozen instantly.

 Remove the app from the device: If the victims had any third-party apps installed, log out of them, and delete the application to stop scammers from accessing saved credit card details in the app.

 Hire fund recovery experts: Hiring fund recovery services is also another option to ensure funds from scammers can be recouped.

How Fund recovery services can help recover lost funds?

Hiring fund recovery is a logical approach that scam victims consider when they feel they require expert help. These services match their business goals to meet the victims' requirement. These services are equipped with a team of investigators, lawyers, retired cyber security officers who have been working in the cybersecurity field for years.

They extend their services into building workable solutions beneficial for scam victims and get them justice. In addition, they eliminate the roadblocks in the way of fund recovery.

Fund recovery companies also align crime detection efforts by collecting relevant evidence to bring criminals to justice.

Thus, it is vital to identify a dependable and reliable name in the field that can help victims abate

the financial crisis as well.

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
