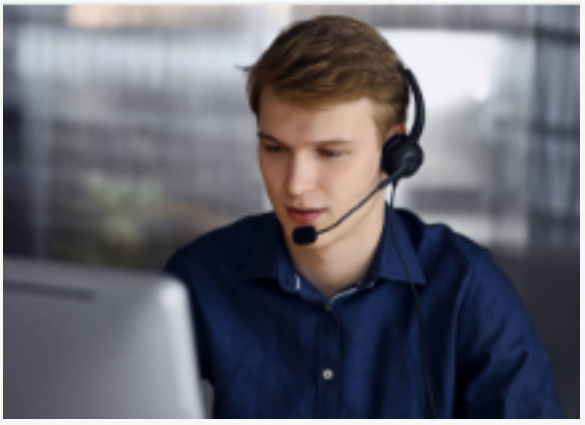
Fraudsters Target Loyalty Programs To Collect Personal Information: Cyber-Forensics Explains About Loyalty Scam

Loyalty programs deliver ample amounts of information to businesses and scammers try to access this information ,and use them to commit identity theft.

Cyber-Forensics.net



Cyber Forensic Specialist

SOFIA, BULGARIA, August 31, 2022 / EINPresswire.com/ -- Digitalization has taken over the world in a blink, and with the help of the internet, it has been easier for businesses and companies to grow and reach out to their customers. But staying at the top without losing customers is a tough job for a business or company. People have hundreds of choices and take no time to close the deal.
Businesses or companies offer loyalty programs with discounts, rewards, and other special incentives to add new customers and retain old ones. But as we know, fraudsters are lurking all over the internet. They target people and lure them into sharing their details to exploit points.
They even target such programs to collect their customers' information.

According to the Federal Trade Commission, "they received reports from 96,000 people targeted by well-known e-commerce market platform impersonators, and nearly 6000 people said they lost their money. Reported losses topped more than $27 million."

Cyber-Forensics.Net, a bitcoin scam recovery company, says, "The scammer uses the phishing technique to execute loyalty points fraud. They send emails to the customers claiming to be sent by a well-known business or company and ask the customer to verify certain account information. After the scammer gets the credential information, they drain the customer's account by redeeming the points or transferring them."

What Is A Loyalty Fraud?

Loyalty fraud is a scam where the scammer abuses or exploits a merchant reward program for nefarious purposes. The most significant opportunity for scammers is monetizing collected

loyalty data and points.

> “Fraudsters often pose as a member of legitimate organizations and reach out to people and convince them to click on the fake website link and share their personal information.”
>
> *Timothy Benson*

According to research, loyalty program-related fraud has risen 89 percent yearly, with approximately $1 billion in rewards value lost to loyalty fraud annually.

What Are The Different Loyalty Scams And How To Identify Them?

 Phishing Attacks: The first step of loyalty program fraud begins with the hijacking of members' accounts. To obtain these personal and financial details, scammers often pose as government or organization officials and send spam emails that provide a link to the scammer's account. Instead of going to the legitimate loyalty program website, the victims are directed to phishing websites that steal their personal information, username, and password.

 Database Thefts: Fraudsters even target loyalty programs directly to steal their member's financial and personal information. The scammers use unpatched software to make their way into loyalty program databases and extract their members' data.

 Account Takeover(ATO): Here, the scammer hacks into an account by using the member's stolen personal identification number or by collecting their details through cyber-attacks like phishing scams and exploiting points balances and payment details attached to the account.

 Policy Abuse: This may be performed by legitimate loyalty members. They identify a way and exploit loopholes to earn many points or rewards using the platform or the program terms and conditions.

 Pooling Fraud: Also known as new account fraud, the scammer creates a fake account by using stolen personal information and then uses the version to sell and redeem misappropriated points. The loyal program allows its members to transfer points from one account to another, which is a helpful feature but equally helpful for fraudsters.

How To Stay Protected From Loyalty Scams?

Timothy Benson, a chief analyst at Cyber-Forensics, says, "The most common way a scammer uses to execute loyalty points fraud is by phishing attacks.
Fraudsters often pose as a member of legitimate organizations and reach out to people through emails and text messages, convincing them to click on the fake website link and share their personal information."

The fraudster uses the phishing attack technique to execute loyalty points fraud. In many cases,

the scammer sends an email to be sent by hotels or travel agents and requests the customer to verify certain account information. They use graphics from renowned companies and pretend to be them. Scammers know that people are naturally more protective of personal banking information than their loyalty program info; that is why consumers are more likely to fall for this trick.

However, there are many things consumers and companies can do to prevent loyalty fraud:

 If a customer's account is inactive for a long time and suddenly becomes active. Verify the customer by asking for security information before accessing their account.
 Request customers to create a unique and robust password combining numbers, special characters, and letters. Remind them to change their passwords.
 Check for spelling errors on the website, and you will avert an immense tragedy.
 When receiving an email, one should double-check the sender's email. Scammers use a different word in the domain name, which might not be visible at first glance.
 Taking a second opinion on a fishy email or contact can save you from taking any wrong steps.

What Is A Fund Recovery Company?

A fund recovery company is a team of professionals that helps an individual recover their lost funds in online scams. They offer services to customers worldwide with their years of knowledge and experience. These professionals have been trained to spot fraudulent behavior and are well-versed in scammers' tactics. They have exclusive tracking technologies that help track down fraudsters with the help of authorities, even if they try to hide their identity through various exchanges and currencies.

Beware of Fund Recovery Scams.
A funds recovery scam is one that pretends that they will do the work but just steals the money. They are typically fly-by-night operations with brand new websites and little web presence or news, demanding cryptocurrency deposits and communicating by generic Gmail and yahoo emails rather than established companies. A bitcoin recovery expert cost s money, but they will not charge the fee in cryptocurrency.

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