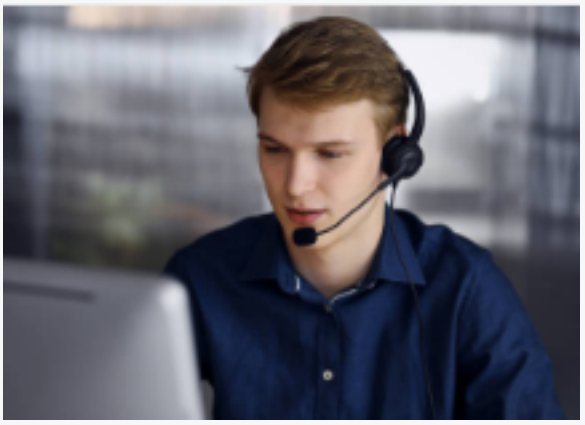
Overpayment scams are back: Cyber-Forensics.net says to be careful when receiving/sending money

In overpayment scams, tricksters pay extra amounts via a fake check to obtain a service and later, put pressure on the service provider for the excess amount.



Cyber Forensic Specialist

Cyber-Forensics.net

SOFIA, BULGARIA, January 31, 2022 /EINPresswire.com/ -- An emerging trend in cyber crimes is becoming a growing cause of concern for authorities worldwide. Scammers are giving a new twist to a classic banking scam called the overpayment scam.

Cyber-Forensics.net, a cyber forensics service for online scam victims, has studied the history of overpayment scams since the last decade. The observations reveal that overpayment scams have made their comeback in recent weeks since 2004.

Fraud recovery specialist at the same firm, Timothy Benson, gave a working insight into how the overpayment scams work:

How does the Overpayment Scam work?
A stranger responds to a service posted online and offers to pay via fake check. At the last minute, the so-called service obtainer comes up with why they have paid the service provider more than the purchase price. The service receiver asks the provider to wire back the extra part of the funds paid mistakenly.

Scammers use words like "Cashier's check" or "Certified check" to make the scam more believable. But the check is counterfeit. Later, the check bounces, leaving the seller liable for the entire amount plus losing the money that the service provider wired back to the fake service receiver.

Benson says that there is a need for consumers to understand that "just because a check has 'cleared' does not guarantee the issuing bank has deposited that money. Sometimes it may take days or even weeks to discover that the check is counterfeit. Consumers often tend to ignore all

> A typical pattern in overpayment scams is to force the victim to send money before the check bounces. They're especially common in job ads, sale items."
>
> *Timothy Benson*

the red flags which they shouldn't."

But while in most cases where potential targets tend to miss such red flags, Ashley Morgan deposited a $3,000 check despite noticing all the red flags.

What happened?
The Brazos Valley musician received a fan request in August 2021 for composing a custom happy birthday song for $500 as payment.

The fan cum scammer agreed to pay $300 before work and rest after completing the work. But things soon took a wrong turn. The singer remembered, "He sent a check from his business account. Then he said he accidentally cut a check for $3,000 instead of $300. So, they wanted $2500 back.

Morgan gave in to the pressure that the scammer built, and she ended up depositing $3,000. After weeks, when her check didn't clear, she understood that she was just scammed.

Timothy Benson, the chief analyst with Cyber-Forensics.net, says, "A typical pattern in overpayment scams is to force the victim to send money before the check bounces. They're especially common in job ads, sale items. One should pay extra attention to avoid such scams.."

How to avoid check overpayment scams?
Know the person sending the check: In any transaction, ensure to confirm the independent service requirer's identity by doing a background check on their name, street address, phone number.

Never accept a check for more than the item's selling price: Ask the individual to check the amount being sent for the desired product or service. If the buyer refuses to send the correct amount, return the check and never send the merchandise before accurate payment has been agreed on.

Consider an alternate payment method: Individuals can consider escrow or online payment services. If the buyer insists on using a particular payment channel, check it before using it. Visit official websites and read about the terms and conditions of that particular service. Call customer service. If satisfying answers aren't available, get the buyer to agree using a reliable payment channel.

In case of payment by check, ask for a check drawn on a local bank/ local bank branch: By ensuring to receive check payments in a local bank, service providers can physically check the validity of the payment.

End the transaction immediately when someone insists on back wiring funds: Avoid the urgency to act immediately.

Resist the urge to enter any unknown lotteries: According to experts, most foreign lottery solicitations are phony. It is illegal to play any foreign lottery.

Can someone get back money lost in check overpayment scams?
Most payment methods sent to scammers cannot be reversed. However, finding scammers, bringing them to a lawsuit, and recovering money is possible with a few exceptions. A Cardinal Rule: Report the matter to cyber experts. A victim's best hope in such cases is involving cyber experts. The experts are familiar with the bank or company payment systems.

Along with ensuring maximum fund recovery, cyber experts also provide emotional support by presenting the honest status of fund recovery company' procedures.

If there's an unknown payment from the account:
Contact bank immediately if:
There is any unrecognized/Unauthorized bank payment
The amount debited from the account is more than the item bought/sold for
Explain the details of the scam and ask to get a refund.

Speed is the Essence:
The consumer's chance of recovering their money lost in scams is stronger when complaints are reported quickly to both: cyber experts and law enforcement such as Cyber-Forencis.net, FBI, FTC, Interpol, Local police, etc.

Fund recovery company advise necessary steps to be taken depending on the nature of the scam and the payment's scale.

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. Cyber-Forensics.net commonly deals with bitcoin scams and forex withdrawal problems. For more information, please visit https://cyber-forensics.net/.

Peter Thompson
Cyber-Forensics.net
+1 917-920-6613
email us here