**Amazon scams 800 S4**

**Introduction**

Is there really a rise in Amazon scams? In any case, if you've had experience, it's not unusual for the topic of scamming to come up frequently in various places. When we dug deeper into this, we found a few vendors who had gotten some strange calls, emails, and even an inquiry. While you would think that scammers are only demands for transfers of money, they can be much greater. New Amazon sellers appear to be the prime target of scammers these days. So, if you're just getting started, could that be you?

Cybercriminals are proving to be extremely smart. They mislead any buyer using smart and convincing language in their emails. Scams are not a modern thing. They've been around for quite a lot longer. Each day, new and imaginative fraud or vulnerabilities are found and handled.

**1. Scam of unauthorized purchasing**

In this situation, a person will get a malicious email or a phone call regarding an expensive transaction made without their knowledge from their account. The email usually includes a fake link to Amazon's website or a phone number to contact with queries about the purchase. When customers click on a link or phone a number, hackers acting as Amazon employees will say that they require their credit card details to halt the transaction and cancel the purchase. Of course, if you give over your information, they will immediately drain your bank account.

**2. False tech support**

Such fraudsters can phone users directly or encourage customers to interact with them via a fake email saying that there is a problem with their account. They then can convince people to install hacking tools or software to tackle the problem.

**3. Links to fake links**

This is generally in the form of an email or an SMS message. It may appear to be a genuine Amazon notification, asking you to click on a link and log in to your account to resolve a problem. However, the website you're visiting is controlled by hackers, and now you've revealed your Amazon credentials.

**4. Scam using gift cards**

A gift card scam occurs when hackers trick users into purchasing Amazon gift cards and disclosing their credit card details. The gift vouchers can then be instantly cashed by hackers. Because numbers are just one, the buyer can no longer use them.

They can come up with different of such scenarios to convince you to buy the cards. Scammers may act as your colleagues or family members, claiming that they have forgotten their wallets and must make an emergency Amazon purchase. They may also mention that you or someone in your family is in financial trouble and needs cash help in the form of gift cards. In other cases, hackers can create fake donation projects which collect gift cards as donations. All these are a few samples of possible outcomes. Hackers generally push people to react quickly in these cases. Messages usually get a sense of urgency. But please remember that Amazon gift cards do not act as money, and real sellers usually never receive them as payment.

**5. Payment scamming**

Payment scams are often simple: hackers seek to convince you to pay for your goods from outside Amazon's secure platform. They offer various discounts or gifts if you pay through Money Transfer, Money Gram, PayPal, or bank transfer. But, if you trust their claims, you would not receive your money or the goods you ordered. Such sellers will delete their accounts immediately after. Amazon would be unable to help you because the payment was made from an outside company system.

**6. Scam of failed delivery**

This is an old online fraud that targets honest sellers. It's simple: a customer says they didn't receive an order and demands a refund while they did. This issue is easily solved by using track-and-trace payment. It means that no goods may be delivered unless the receiver pays for them.

**7. Prize fraud**

Now, this comes in the form of a message informing users that they have won a prize but must click on a malicious link to get it. Of course, the Web address is operated by criminals who will either attack you with software or collect your information.

**Conclusion:**

The phrase "trust but verify" is still applicable to internet commerce and its connected activities. In conclusion, the majority of scams may be avoided if you exercise caution, ask questions, and have your wits about you. Never provide personal sensitive information to anyone posing as a "customer service representative or agent" if you receive any unsolicited emails; instead, be extra careful to investigate their source.

**FAQs:**

**1) How to identify if the message I received is a scam or not?**

Amazon has clarified that it doesn’t anonymously send password reset or account verification emails. They request us not to provide any information on credentials and to not open any links in those kinds of messages.

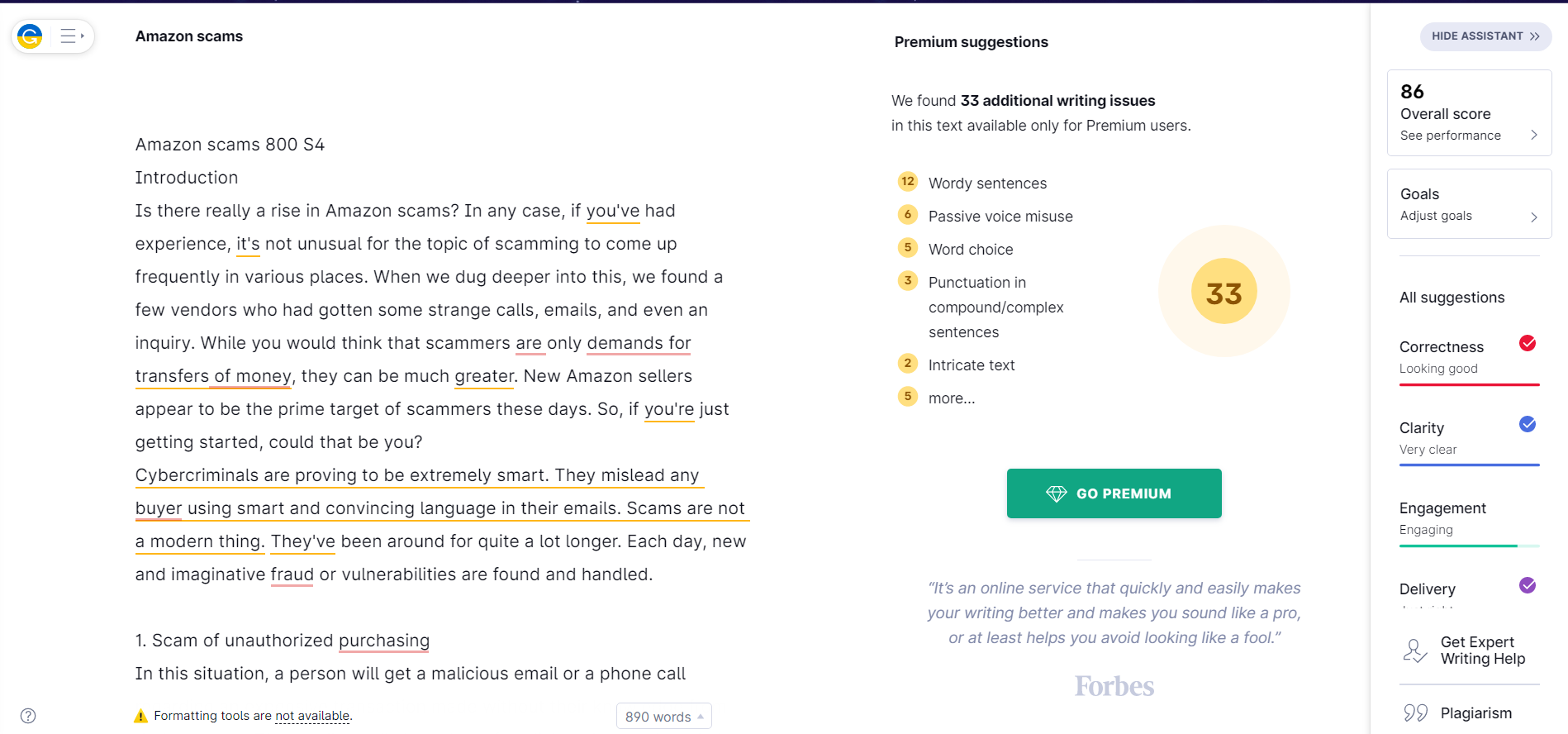
**2)** **Where to report such scams?**

We can report any suspicious activities to Amazon customer service. They will guide us for further actions to be taken.

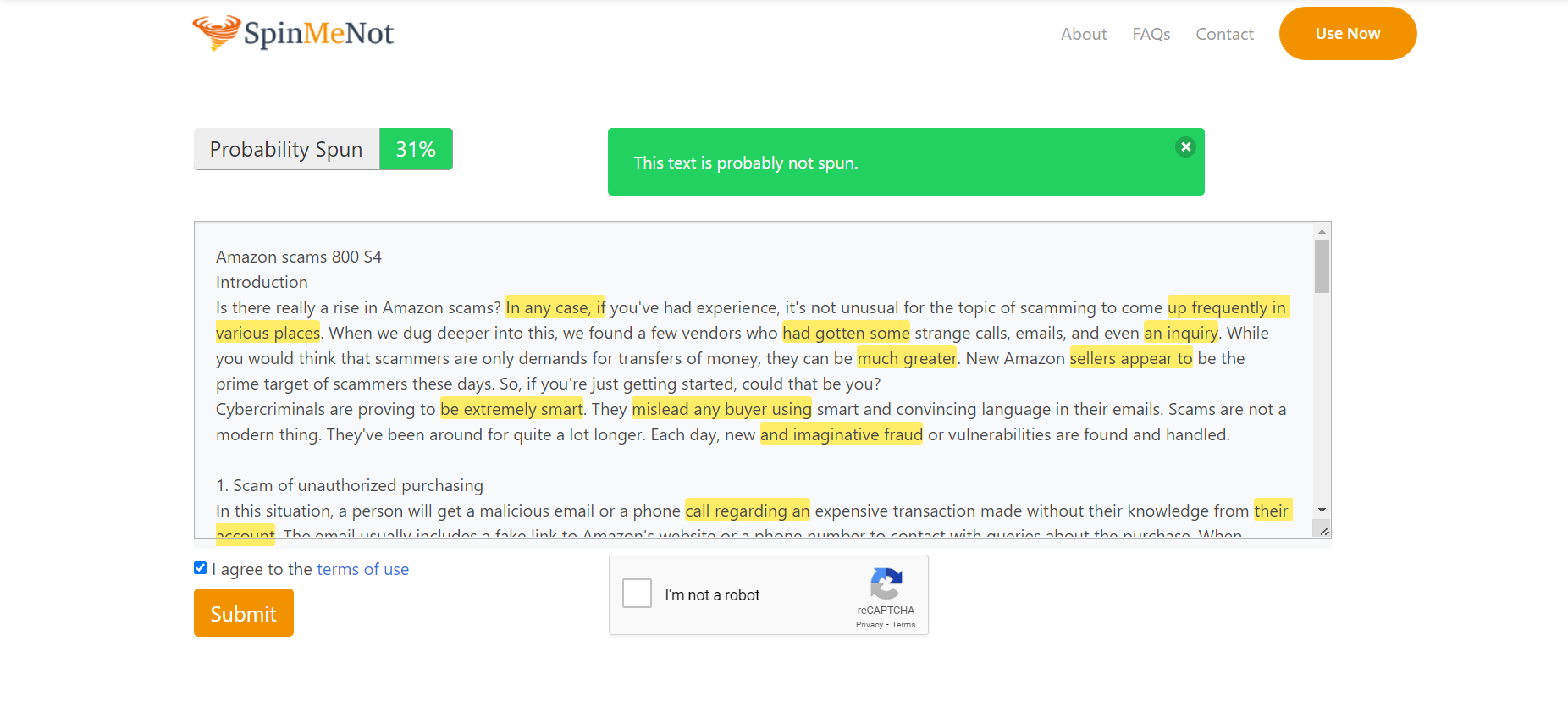
**3) Are all those gifts and lottery messages from Amazon fake?**

Yes, they are fake and they are not from Amazon. Amazon has confirmed that they never send those kinds of messages to their customers so be aware of those scams.

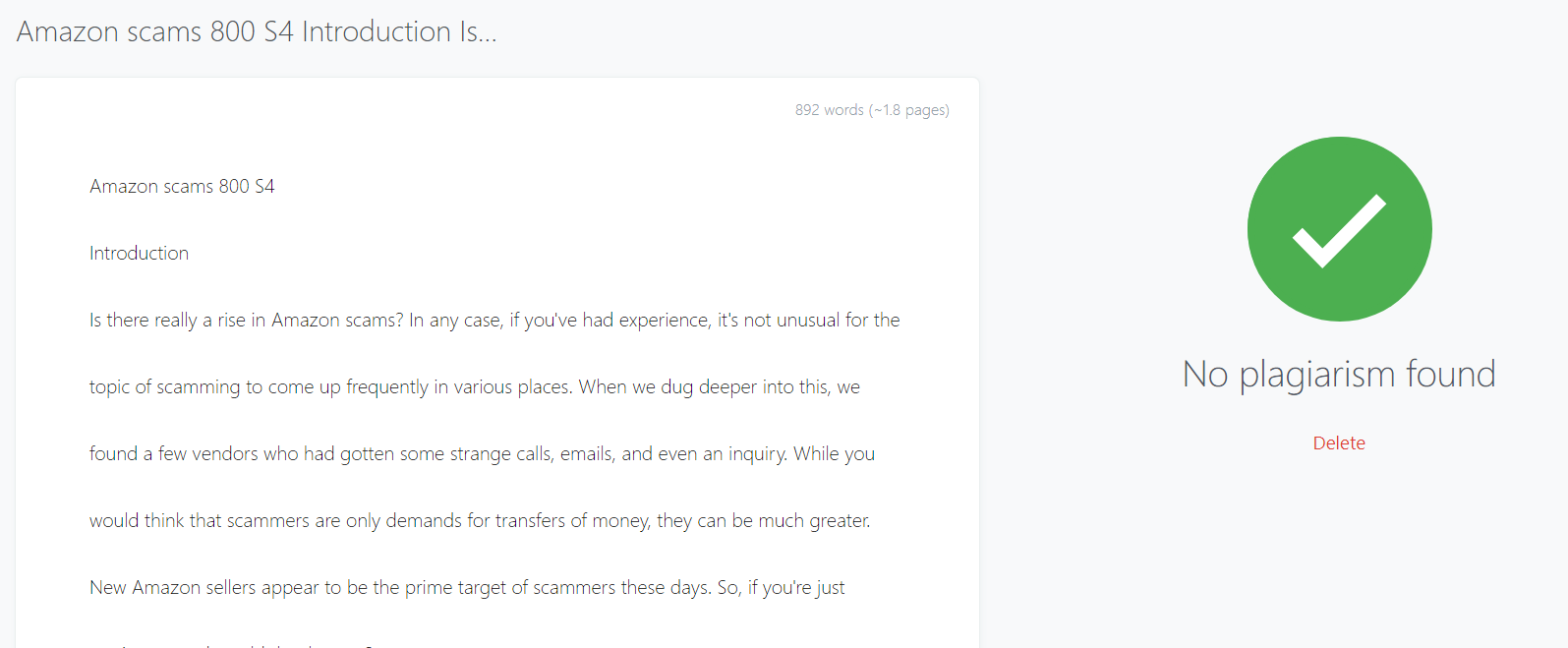
**Grammarly screenshot:**



**Spinmenot screenshot:**

****

**Quetext screenshot:**

****