Paul Roseway 2127271

Avoid online scam

Phone call

- Why this buyer offering more money for the sneakers,
- Why the buyer did not want to use the action website because of service fees.
- Instead Of buying it from the action website she wants to buy it directly from the seller himself,
- On the call the buyer sound like she was in a hurry,
- She also wants the seller to ship the sneakers overnight because it is urgent.
- Hope Kamar gets paid before sending the sneakers.

Email/Receipt:

- How did the buyer get Kamar email address and phone number something not right,
- Kamar was very careful sending his payment details to the buyer online or any login details,
- Kamar received an email confirming the payment from the payment service, but something does look right,
- Kamar should not send the sneaker before having a good check on everything, making sour all details are ok before sending his sneaker.

Should Kamar ship the shoes

- If the buyer pays for the sneakers and all is good, then Kamar should ship the sneakers.
- Before Kamar ships the sneakers, he should check if all details are correct, and the payment details are also correct then ship the sneakers.

Kamar should not send the sneakers

- His account should also show that the payment arrived, and the payment website should email Kamar to tell him that he was paid.
- Kamar should not go through using an unprotected website to sell his product.

Decision: didn't ship the sneakers

- Kamar should not ship the sneakers, because the payment was a sense right,
- The buyer call to speak to the seller that seems suspicious,
- The buyer wants to buy the sneakers without using a safe website. That's a red flag.

Paul Roseway
2127271

Online Research,

How to spot a scam

- Phishing emails are often sent in bulk and are unlikely to contain both your first and last name, they commonly start: ‘Dear Student’.
- Check the quality of the communication - misspelling, poor punctuation and bad grammar are common signs of bogus emails or text messages.
- Fraudsters will try to create a sense of urgency as a way of pressuring you into giving your personal details. For example, they’ll say things like ‘failure to respond in 24 hours will result in your account being closed’.

How to avoid these scams

- Keep an eye out for any emails, phone calls or SMS messages you think are suspicious, especially around the time you’re expecting a payment.
- You shouldn’t post messages online that let people know you’re getting your student finance payment soon; this could make you a target for fraudsters.
- Always ensure that you’re using a secure website when submitting sensitive information online and don’t post personal info on social media pages.
- Avoid logging in to your student finance account on public networks or computers.

How to avoid these scams

1. Personal information, like your Social Security, bank account, or credit card numbers. If you get an email or text message from a company you do business with and you think it's real, it's still best not to click on any links. Instead, contact them using a website you know is trustworthy. Or look up their phone number. Don't call a number they gave you or the number from your caller ID. Resist the pressure to act immediately. Legitimate businesses will give you time to make a decision. Anyone who pressures you to pay or give them your personal information is a scammer. Know how scammers tell you to pay. Never pay someone who insists you pay with a gift card or by using a money transfer service. And never deposit a check and send money back to someone,
2. Scammers often pretend to be contacting you on behalf of the government. They might use a real name, like the Social Security Administration, the IRS, or Medicare, or make up a name that sounds official. Some pretend to be from a business you know, like a utility company, a tech company, or even a charity asking for donations. They use technology to change the phone number that appears on your caller ID. So the name and number you see might not be real.
3. Scammers say there's a PROBLEM or a PRIZE. They might say you're in trouble with the government. Or you owe money. Or someone in your family had an emergency. Or that there's a virus on your computer. Some scammers say there's a problem with one of your accounts and that you need to verify some information. Others will lie and say you won money in a lottery or sweepstakes but have to pay a fee to get it.
4. Scammers PRESSURE you to act immediately. Scammers want you to act before you have time to think. If you're on the phone, they might tell you not to hang up so you can't check out their story. They might threaten to arrest you, sue you, take away your driver's or business licence, or deport you. They might say your computer is about to be corrupted.

Email Draft to Report a scam

How to report a scam

- Reporting a scam helps track down and stop scammers. This prevents other people from being scammed,
- Cyber criminals use fake messages as bait to lure you into clicking on the links within their scam email or text message, or to give away sensitive information such as bank details.
- If you have received an email which you're not quite sure about, forward it to the Suspicious Email Reporting Service, *report@phishing.gov.uk*
- Contact the police immediately by calling 101 if the scammer is in your are area,
- If you feel threatened or unsafe call 999, Gather all the details of the scam,
- Write down the details of your scam. This will help you remember all the important information when you report it.
- who you've been in contact with write down names, numbers and addresses if you have them,
- why you're suspicious,
- what information you've shared, passwords, PINs, or bank details,
- whether you've paid any money,
- how you've paid for example, credit card or bank transfer.

Draft Email

Dear Fraud Support Team

I’m writing to report a online scam on your sales websited, I have be using your sales website from the past ten mounts. I was selling an item to a buyer on E-Commerce. The sales number 83961853, I listed the item on monday while going through my emails I received a call from the buyer, saying that she would like to speak to me concerning the sale. She told me that she would like to buy the sneakers but off the site. I was questioning myself why she wanted to buy it off the site. But then she tried to convince me to send the sneakers overnight. I Sent her a payment request on the pay money app.
I got an email from a weird email address with a pay money receipt. It had pay money logos but it looked like a fake receipt, I didn't get any direct payment message confirming the payment, when I checked my account there was no payment sent for the goods.
But when I found out it was a scam I blocked her and stopped communicating with that person.

If you need more information please let me know. I can provide you with all the chats and messages, also the phone call and number.

I hope this will help you to catch the scammer and stop her from scamming others.

Thanks Paul Roseway,