This Refund Costs Money

In this week's scam, you receive an email that appears to be from Microsoft. The email says that you have purchased a subscription to one of Microsoft's products. It seems legitimate because it is sent from a Microsoft domain, has a genuine order number in the text, and even contains official logos.

The email claims that you bought an expensive Microsoft subscription and gives a number to call for a refund if you didn't make the purchase. But this email and the support phone number aren't real. If you call the number, scammers posing as Microsoft support will likely ask you for your login and bank account information. You never actually paid for any Microsoft products, but if you call the fake phone number, you will pay the scammers!

Follow these tips to avoid falling victim to a phishing scam:

- You should always be suspicious if an unsolicited email asks you to call a phone number. Microsoft would never request that you call a phone number for a refund.
- If you have concerns about a purchase, always go directly to Microsoft's official website.
- Always be cautious when you receive unexpected emails about account problems, security alerts, or purchases. These emails can be a setup for a phishing scam.