Look Out for this Two-Step Cyberattack!

Vishing or "voice phishing" is when a cybercriminal tries to convince you to give sensitive information over the phone. Typical vishing involves only a phone call. But scammers are now combining emails and phone calls to better trick their targets.

Here's How it Works

1 The Setup

You receive an email claiming that you've purchased an item or authorized a payment. You're encouraged to call a phone number if you did **not** initiate the transaction.

2 The Takedown

You call the provided number and a helpful agent agrees to provide a refund or cancel the transaction. They just need your credit card information or banking details.

After you supply the information, your bank account is emptied or your credit card is used for fraudulent purchases.

What You Can Do

Look for these red flags. If you see any, it's probably a scam!

Generic email address

From: **Orders <GenericEmail@gmail.com>**
To: **Jamie Doe**
Subject: **Your Order**

Thanks for your order! It is being processed and will ship soon.

You didn't make the transaction

Order Date: 01/01/22
Payment Type: Credit Card
Amount Paid: $542.12

You're asked to do something you've never been asked before

If you did not place this order, please call Customer Service at 888-###-#### within 24 hours to cancel.

Pressure to respond

Never call the number in a suspicious email, even if you do business with the referenced organization! Call the Customer Service number on the organization's website and ask about the transaction described in the email.

KnowBe4