KnowBe4

Security Hints & Tips

Unexpected Emails

Many of us receive a steady flow of emails every day, including bank statements, order confirmations, or sales promotions. To keep up, you may look through your inbox as quickly as possible—but don't forget to stay vigilant. Cybercriminals take advantage of full inboxes to send dangerous, unexpected emails.

Unusual Scam Activity Detected

One of the most popular unexpected email scams includes fake banking emails. Cybercriminals will send you an email that appears to be from a local bank, claiming that they have suspended your account due to unusual activity. Before taking action, consider whether it makes sense that you're getting this email. Ask yourself questions like:

- Do you have an account with this bank?
- Is this how your bank typically contacts you when unusual activity is detected?
- When was the last time you checked your bank account?

If you don't stop and think, you may give cybercriminals exactly what they want.

Your New Scam Is on the Way

In another scam, cybercriminals imitate a popular retailer's order confirmation email. The email states that your card was charged a large sum of money and your order is on the way. Even though a fraudulent charge is alarming, pause and determine if the email makes sense. Ask yourself questions like:

- Do you shop at this retailer?
- Have you ever entered your credit card information on their website?
- Does the email include any accurate identifying information, like your name, credit card number, or shipping address?

Without pausing to ask yourself questions like these, you may fall right into a cybercriminal's trap.

The KnowBe4 Security Team
KnowBe4.com

What Can I Do to Stay Safe?

Follow the tips below to stay safe from unexpected email scams:

- When you receive an unexpected email, stop and consider the context. For example, if the email is about an order you didn't place, it could be a scam.
- Never click a link in an email that you aren't expecting. Instead, open your internet browser and navigate to the organization's official website.
- Watch out for urgent messages, such as an email alerting you about an expensive credit card charge. Phishing attacks rely on impulsive actions. So, always think before you click.