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.

KnowBe4

Security Hints & Tips

Unsafe Email Attachments

Many people use email in their personal life and their workplace. You can get an email from your aunt with her stew recipe or an email from your boss with a guest list for the office party. But what if the email isn't actually from your aunt or boss? Cybercriminals often pretend to be someone you know to get you to click unsafe attachments, such as fake DOC files or PDF files. Some of the most common attachments used for attacks are DOC files and PDF files. It's important to learn how to identify unsafe email attachments and protect yourself.

Fake DOC Attachments

Older Microsoft Word DOC files are commonly used in cyberattacks because they can include macros. A macro, short for macroinstruction, is a set of commands that can control a DOC file and other programs. Cybercriminals may send you an email with a DOC file that contains a macro. The email usually looks legitimate and gives an urgent reason for you to open the file. If you open the file, a pop-up window will display asking you to enable macros. If you accept, the macros will be able to install malware on your device.

Fake PDF Attachments

PDF files are sent over email every day, making them perfect tools for cyberattacks. One popular type of attack is when cybercriminals put an image in a PDF file to trick you into clicking it. For example, it could be an image that looks like a video with a play button. The image will be something that catches your attention, like a cooking video from social media or a cute cat video. Unfortunately, clicking the image could send you to a website designed to steal your sensitive information.

The KnowBe4 Security Team
KnowBe4.com

What Can I Do to Stay Safe?

Follow the steps below to stay safe from dangerous email attachments:

- If a suspicious email appears to be from someone you know, contact them over the phone or in person. Check to see if the email is legitimate before putting yourself at risk.
- Avoid DOC files in general. They use an outdated format and contain too many security risks. The newer DOCX format is the current standard and is much safer.
- Always think before you click. Cyberattacks are designed to catch you off guard and trick you into clicking impulsively.