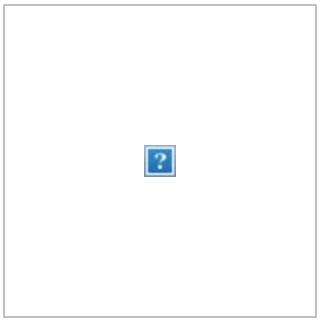
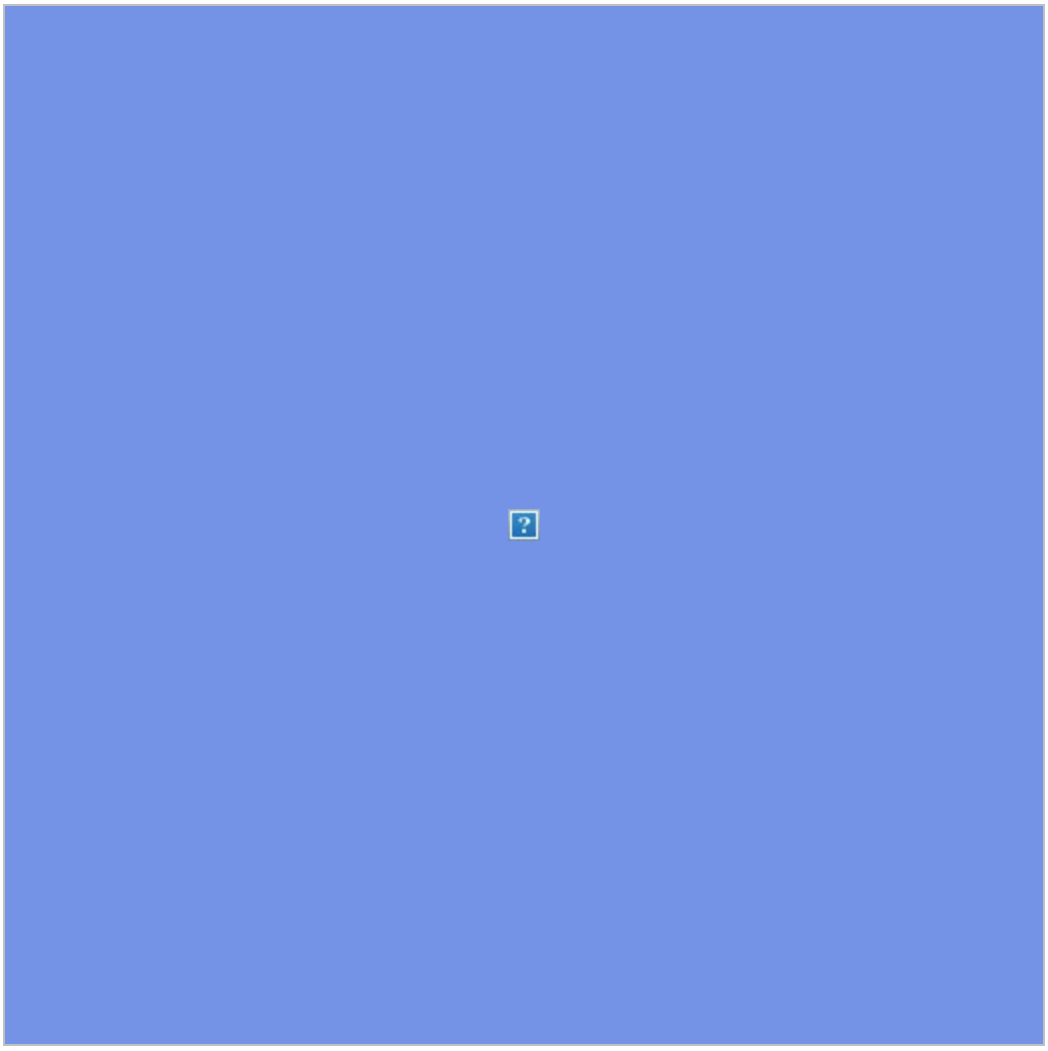
From: do-not-reply@knowbe4.com
To:
Subject: Scam of the Week: The Microsoft Forms Fakeout
Date: Wednesday, September 18, 2024 9:16:03 AM





Scam of the Week

The Microsoft Forms Fakeout

In this week's scam, cybercriminals are using a tool called Microsoft Forms to try and trick you into giving them your Microsoft 365 or Adobe login information. Microsoft Forms allows you to create surveys, quizzes, and other documents. Unfortunately, cybercriminals are using this tool to create forms that contain malicious links. These fake forms can easily fool you into thinking they're official Microsoft documents because they have convincing titles and even use Microsoft icons when viewed in a web browser.

In this scam, you receive an email instructing you to urgently change your password, read messages, or look at sensitive work documents. The email directs you to the form, prompting you to click a link. However, the link is malicious, and if you click it, you will be directed to a fake Microsoft 365 or Adobe login page. This page will prompt you to enter your sign-in details, such as your email address and password. If you enter your login credentials here, cybercriminals can steal them!

Follow these tips to avoid falling victim to a Microsoft Forms scam:

- Be cautious whenever you receive an urgent request, such as changing your password or viewing sensitive documents. Remember that cybercriminals play on your emotions by forcing you to act quickly.
- Before you click a link, always hover your mouse over it. Watch out for spelling mistakes or suspiciously long URLs that can hide a website's true domain.
- If you receive a suspected phishing email, follow your organization's policies for reporting suspicious emails.

The Coast Community College District Security Team