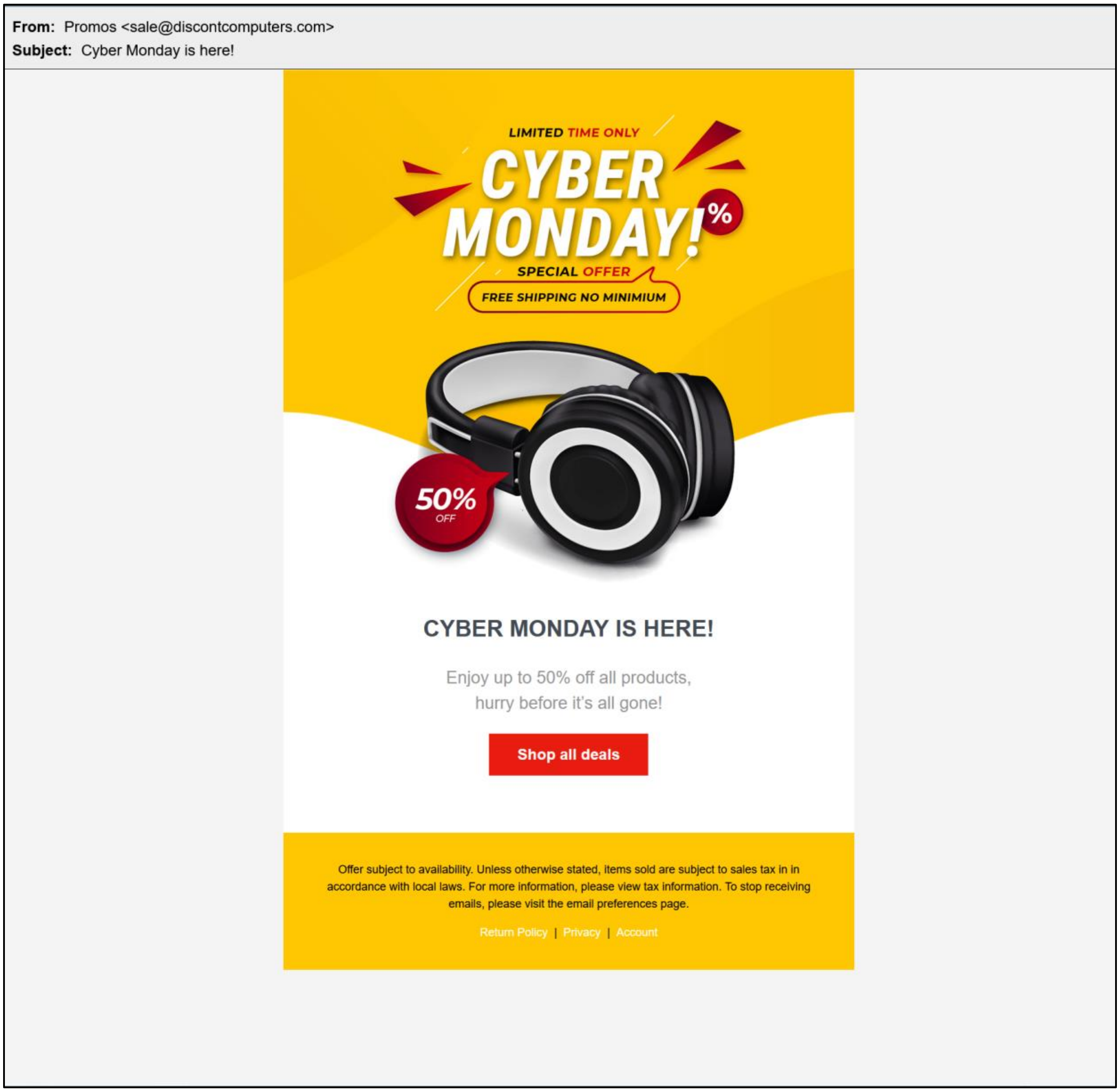
November 2023 Phishing Scenario Results

The Office of Information Technology (OIT) strives to educate the MC community on safe computing habits and security awareness topics to safeguard College and user data. OIT randomly sends simulated phishing email scenarios with the purpose of promoting security awareness and helping users to recognize phishing attempts. Our goal is to achieve zero clicks on real and simulated phishing emails.

The November scenario tested employee susceptibility to holiday shopping deals with a simulated phish titled, “Cyber Monday is here!”



From: Promos <sale@discontcomputers.com>
Subject: Cyber Monday is here!

CYBER MONDAY IS HERE!

Enjoy up to 50% off all products,
hurry before it's all gone!

Offer subject to availability. Unless otherwise stated, items sold are subject to sales tax in in accordance with local laws. For more information, please view tax information. To stop receiving emails, please visit the email preferences page.

The results showed:

247 employees reported the suspicious email.

16 employees clicked on the "Shop all deals" link. That's one click too many.

This is prime season for attackers to send out malicious holiday themed "Cyber sale" or "Delivery postponed" emails and catch employees off guard. Their goal is to trick you into entering your login credentials in a fake online shopping website or worse, provide an attachment for download that is laced with ransomware.

To avoid falling for these tricks remember to pause, reread the email, and if suspicious, report the email using the Report Phishing button. Most importantly, use a personal email address for all personal business especially for personal shopping accounts. This account separation helps you evaluate incoming emails. For example, a "Paypal" email addressed to your MC email address is a red flag.

Concerned the email is related to MC business? The best way to check on your MC business accounts with is to login to your account using the bookmarked web address.

What should you do if you suspect an email may be a phishing attempt?

Let IT Security analyze the email for you - **REPORT** the email! The Report Phishing button within your email client allows you to quickly report suspicious emails to IT Security. Learn how to access the Phishing Reporter button when using Office 365 at home or from a mobile device.

As always, if you have any questions or concerns, please contact the IT Service Desk:

- by email at itservicedesk@montgomerycollege.edu
- by web chat on OIT's web page
- by phone at 240-567-7222