Phishing Results: Online Shopping

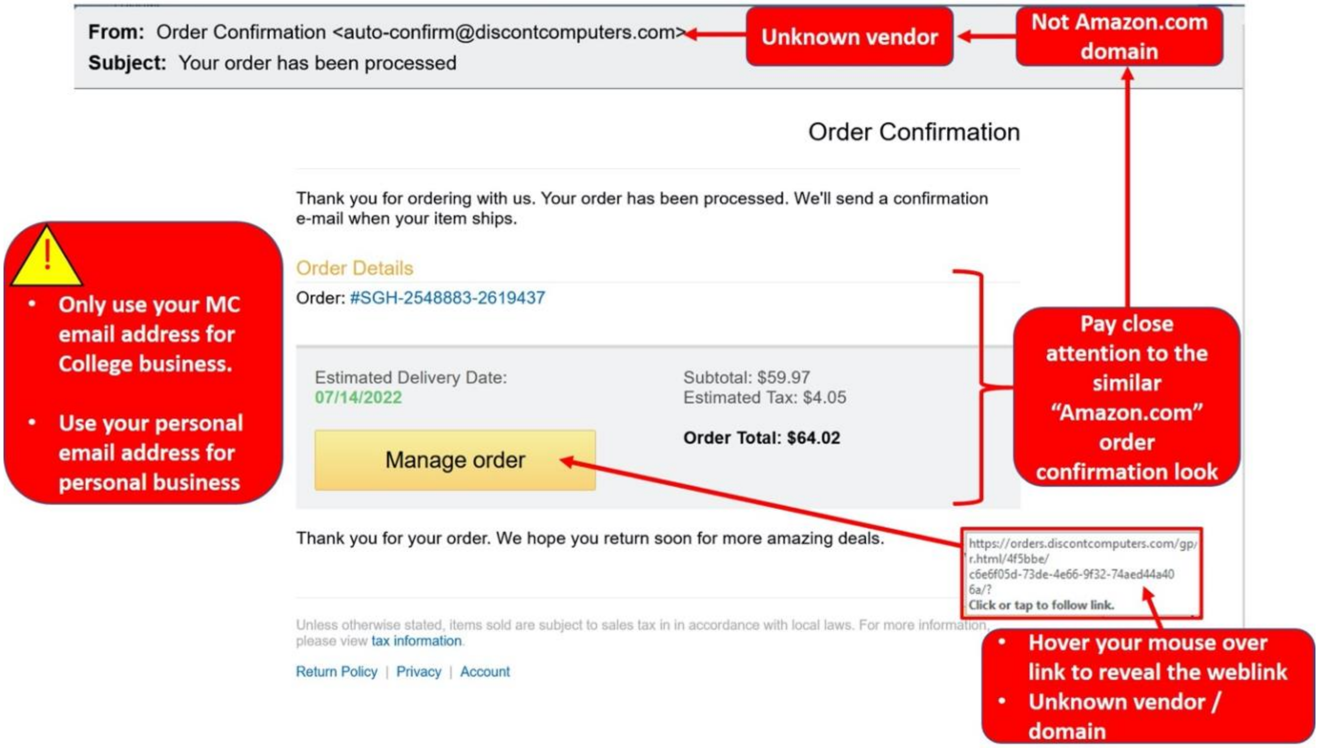
The Office of Information Technology (OIT) recently completed a simulated phishing scenario titled, *Your order has been processed*. This scenario used the familiar online order email to lure employees into clicking the link.

Shopping online is convenient and provides the consumer with a barrage of order and shipping updates via email. The multiple email notifications from multiple vendors can be difficult to discern which emails are legitimate. Many shopping order scams start with an email with a malicious link to include a message to "manage your order". While these messages often look or sound legitimate, you should never click the link. Instead, review your orders by contacting the vendor directly by using a verified number or website.

936 employees reported the phishing scenario to the Phishtrap. **Nice work MC!**

169 employees clicked the link within the training email. Did you click? In a real-world phishing attack clicking the link may have prompted you to give up your account login credentials.

Please review the clues and tips within the email to help you identify this message as suspicious.



From: Order Confirmation <auto-confirm@discontcomputers.com>
Subject: Your order has been processed

Order Confirmation

Thank you for ordering with us. Your order has been processed. We'll send a confirmation e-mail when your item ships.

Order Details

Order: #SGH-2548883-2619437

Estimated Delivery Date: 07/14/2022

Subtotal: $59.97
Estimated Tax: $4.05

Order Total: $64.02

Manage order

Thank you for your order. We hope you return soon for more amazing deals.

https://orders.discontcomputers.com/gp/r.html/4f5bbe/c6e6f05d-73de-4e66-9f32-74aed44a406a/?
Click or tap to follow link.

Unless otherwise stated, items sold are subject to sales tax in in accordance with local laws. For more information, please view tax information.

Return Policy | Privacy | Account

Unknown vendor

Not Amazon.com domain

- Only use your MC email address for College business.
- Use your personal email address for personal business

Pay close attention to the similar "Amazon.com" order confirmation look

- Hover your mouse over link to reveal the weblink
- Unknown vendor / domain

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. If you accidentally clicked on a link or attachment in a suspicious email, contact the IT Service Desk immediately.

Follow these additional tips to avoid phishing scams:

- Only use your MC email address for College business. Use your personal email for personal business
- Always verify! If you know the sender, but the email seems out of context, follow up with a quick phone call.
- Check your emotions. Do not be curious and investigate the link – REPORT the email.
- Trust your instincts. If the email content, sender, and link or email attachment seems suspicious, do not open it. **Play it safe and REPORT it.**

If you have any questions or concerns regarding this process, 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

Please do not reply to this email, as this mailbox is not monitored. Thank you.

IT Communications
Office of Information Technology