

The Office of Information Technology (OIT) recently completed a simulated phishing scenario titled, *Meeting Today-Ref:0831139445*, which prompted you to click on a Zoom meeting link. Cyber criminals target the millions of Zoom users with look-alike phishing email invites to steal passwords and spread malware.

**983 employees reported** the phishing scenario to the Phishtrap! Reporting is the preferred action as it provides IT Security the threat intel it needs to respond.

**123 employees clicked the link within the training email; of these individuals, 37 entered their credentials.** There were several clues within the email to help you identify this message as suspicious. Please review the email again and pay close attention to the red flags:

The diagram shows an email interface with several red callout boxes pointing to suspicious elements:

- Generic meeting subject:** Points to the subject line "Meeting Today-Ref:0831139445".
- Unknown sender from unknown domain:** Points to the sender information "Meeting-Helpdesk841870 <noreply-desk08116394@my.webshar.es>".
- Contact not named; unknown:** Points to the greeting "Hi First.Lastname@montgomerycollege.edu".
- Hover over the link with your mouse – URL is not the same:** Points to the "Join Zoom Meeting" link. A tooltip is shown below it with the URL: `https://mail.my.webshar.es/u/amo3z6ccodm9/login.srf/0e3bd4/4a58ee93-fb3f-4799-b7d5-a94c6f846ad7/?` and the text "Click or tap to follow link."
- Red circle:** Highlights the text "A contact in your directory is inviting you to a scheduled Zoom meeting."

The email body text includes: "Hi First.Lastname@montgomerycollege.edu", "A contact in your directory is inviting you to a scheduled Zoom meeting.", and "Meeting URL: <https://Montgomery College.zoom.us/j/99162500610221> Meeting ID: 714 4288 46881".

### 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](#)

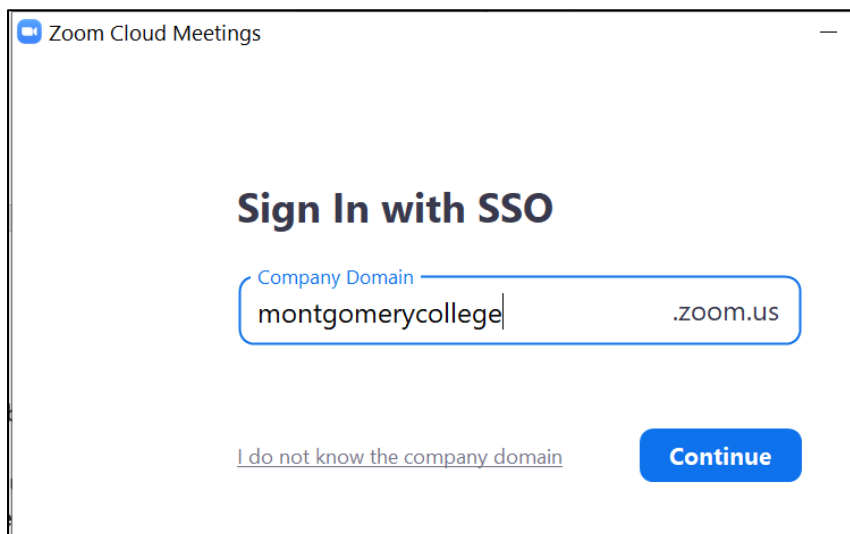
to access the Phishing Reporter button when using Office 365 at home. If you accidentally clicked on a link or attachment in a suspicious email, contact the [IT Service Desk](#) immediately.

### Complete (or revisit) DataSecurity@MC: Annual Review!

**DataSecurity@MC: Annual Review** training provided by SANS will teach you how to better identify common methods used by cyber attackers who try to gain access to account credentials and information systems. The range of training topics takes about 35 minutes to complete and can be accessed in MC Learns through Workday under the **MC Required Training** category

### Below are some common clues to look for in identifying a suspicious email:

- **Review** the [Zoom Conferencing Software webpage](#) to understand how to secure your session, join a meeting, and schedule a meeting
- Do not join or accept random Zoom invites
- MyMC login credentials **are not required** when JOINING a Zoom session
- MyMC login credentials are only needed when accessing your Montgomery College Zoom account!



- 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.
- Be cautious. Malicious actors and aggressive spammers are attempting to take advantage of our new normal by **preying on our stress levels and hoping our guard is down with COVID-19**, gift card, meeting invites, shipping notices, and stimulus check scams.

- 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](mailto: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