

## External email warning banners begin this week

### What is an external email warning banner?

EEH is rolling out an email security warning banner that will be contained in the “Subject” and in the body of the email to warn users that the email they received was sent from outside the organization. **In the case of emails you receive through Doc Box and Board Effects, even though these messages are initiated by Edward-Elmhurst Health, they will still contain the warning message since the platforms we use are from an external source. You should however continue to open your Doc Box and BoardEffects emails.**

### What will this look like?

In the “Subject” of the email, you will see **[EXTERNAL]** added at the beginning of the subject line. See below as an example:

**[EXTERNAL]** Webinar: Understanding Psychology to Improve Cybersecurity

In addition, the following banner will appear at the top of the body of the email:

**CAUTION:** This email originated from outside of the EEH corporate network. Do not click links or open attachments unless you validate the sender and know the content is safe. Please forward suspicious messages to [spam@eehealth.org](mailto:spam@eehealth.org) for review.

### Why is this happening?

IT Security continues to improve upon ways to protect EEH users from phishing and spam emails that may potentially put EEH at risk of a security breach. The intent of this enhancement is to make the end user aware that the email they are viewing did not originate from EEH, and to be cognizant of suspicious or potentially malicious emails.

### When will this begin?

You will see these banners appearing in external emails that may be sent to you, beginning the week of March 8.