Be a Security superhero

EMAIL SAFETY: DO YOUR PART!
Recognize “phishing” and avoid malicious emails. Be suspicious when...

- The email includes the UF Health alert warning.
- You did not expect the email, even if you know the sender.
- You do not know and trust the source.
- The sender’s account appears suspicious. (When you hover over the sender’s name, it shows the full email address is not from a source you recognize or trust.)
- The email asks for personal information or log-in credentials.
- The email is generic and looks like it’s also sent to other people you don’t know.
- It is poorly written with bad grammar and/or spelling.
- It promises a gift or reward for your response.
- It seems urgent, telling you to immediately respond and/or provide information.
- It includes a link you don’t recognize. When you hover over the link without clicking it, it shows an unfamiliar URL/web address.

DO NOT open or interact with suspicious emails!

- If you know the sender an email that looks suspicious or asks you to provide personal information, call the known sender to confirm the email is legitimate.
- If you don’t know the sender or suspect the email is a scam, please report it:
  Gainesville: IT_Security@shands.ufl.edu
  Jacksonville: IT_SecurityJax@jax.ufl.edu

STAY CURRENT ON IT NEWS:
Use the search bar to find “IT Customer Updates” on the Bridge!