What is the mock phishing email simulation and why is the University doing it?

Tell Me

1. A phishing simulation is when an organization sends a mock phishing email to employees. It's designed to help people identify a phishing scam by providing real-time feedback if they click the link included in the phishing email.
2. Actions such as opening the email or clicking on the link are analyzed to evaluate how susceptible the organization is to email phishing campaigns and to guide educational efforts.
3. Mock phishing emails will be sent to faculty and staff, as part of the University’s new phishing simulation program.
4. They will be sent approximately once per month.
5. If you realize it's a phishing email, you can report it to reportspam-group@uncc.edu or delete it.
6. If you fall for the phishing email, you'll be sent to a page that explains you've been phished and offers tips on how to identify a phishing email.
7. You can get more information about phishing emails by contacting your Department's Information Security Liaison (ISL), taking the online Security Awareness Training and/or reviewing cybersecurity best practices.

Related FAQs

- What are the guidelines for storing level 0 - 3 data?
- What is the Security Awareness Training and where can I complete it?
- How do I best secure my personal computer and data?
- What is the policy for employees using mobile devices?
- How do I report an IT security incident?