University of CINCINNATI

SPOT THE HOOK, DON'T GET PHISHED!

COMMON RED FLAGS

1) CREDENTIAL HARVESTING

Cybercriminals frequently send phishing emails that mimic official university communications, such as login portals or library access requests.

2) FAKE JOB OFFERS

Cybercriminals may impersonate university-affiliated employers or internship providers, offering job opportunities.

3) FINANCIAL AID SCAMS

Cybercriminals may send phishing emails or messages impersonating the university's financial aid office.

4) EMAIL ACCOUNT VERIFICATON

Phishing emails from fake university IT departments may request email verification or direct recipients to fraudulent login portals through deceptive links.

5) SCHOLARSHIP AND GRANT SCAMS

Cybercriminals send fraudulent emails offering scholarships, grants, or financial aid opportunities.

6) ONLINE SHOPPING SCAMS

Some phishing emails may imitate online shopping platforms or offer discounts on electronics, textbooks, or other items popular among students and staff.

7) DATA BREACH ALERTS

Cybercriminals might send fake data breach notifications, claiming that the recipient's personal or financial information has been compromised.

8) TECH SUPPORT SCAMS

Cybercriminals impersonate IT or tech support staff and claim that the recipient's computer or account is compromised.

For any Cyber Security questions, please visit the Office of Information Security or email us at infosec@uc.edu