Frequently Asked Questions Regarding Potential Email Scam

When did this event happen?
The issue was identified July 27 by the Controller's Office, which contacted the ITS Department. An immediate investigation began to determine what occurred and its scope.

How can I tell if my information has been compromised?
The University has contacted individuals via email or a phone call if their account was identified as potentially compromised. However, all employees and students using direct deposit should review their information through my.uncc.edu. Individuals who notice any unusual activity should contact the IT Service Desk at (704) 687-5500, option 1.

Should I change my direct deposit account and routing numbers?
Individuals who have reason to believe their account was compromised, should contact their bank and ask about their protocols when fraud is suspected.

How will I get my current paycheck?
Individuals whose accounts were impacted by this issue will still be paid for this pay period; however, because of the compromise, the University will pay them via a paper check.

How will I receive future payments?
The University will continue to issue any reimbursements or payments to impacted individuals by paper check until they have provided correct direct deposit information.

How can I protect my credit?

- The University will offer access to an identity theft protection plan at no cost to anyone whose account was compromised.

- If you have reason to believe your account was compromised, we recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. You initiate this by calling any one of the three major credit bureaus listed below. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. There is no charge for initiating this alert. Additionally, all three credit reports will be sent to you, free of charge, for your review.

Equifax	Experian	TransUnion
888-766-0008	888-397-3742	800-680-7289

Was any other personal information compromised?
While there is no evidence at this time indicating that anything other than the direct deposit information has been compromised, because there's risk that other personal information could have been exposed, we recommend that impacted individuals place a fraud alert on their credit file. Please see the FAQ above for instructions on how to do this.

How can I prevent this from happening again?

- Learn how to identify phishing attempts by reviewing computer security tips on ITS website. You can also access ITS security awareness videos here.

- If you receive a phishing email, please forward it to ReportSpam-group@uncc.edu or call the IT Service Desk at 704-687-5500.
- If you think you've been the victim of a phishing attempt, change your password immediately at pwmanager.uncc.edu or call the IT Service Desk at 704-687-5500 to do this for you.
- For additional security, you can register for Duo, a two-factor authentication system recently announced by the University in this Inside UNC Charlotte article. You can also see this FAQ to help you get started.

Is the University sure this was a phishing scam?
So far, all evidence points toward this being an isolated phishing scam affecting fewer than 50 people, but ITS is still investigating.

Who should I contact if I have any additional questions concerning this security incident?
Please contact the IT Service Desk at (704) 687-5500, option 1.