

From: [All Students](#) on behalf of [Information Technology](#)
To: [All-Students Mailing List](#)
Subject: [ALL-STUDENTS] REMINDER - SCAM ALERT: targeting @g.rwu.edu accounts
Date: Thursday, July 13, 2023 1:47:43 PM
Attachments: [image001.png](#)

Roger Williams
University

Information Security [INFOSEC] Briefing

Phone: 401-254-6363 E-

Mail: mediatech@rwu.edu

SCAM ALERT

We confirmed several email scams targeting RWU Students focusing on summer internships and research projects. Each con varies slightly; however, they typically start with a phishing email, spoofing an RWU professor's name, requesting students to respond with interest for a summer job. Responding to that initial request results in a subsequent email that appears to come from RWU Payroll, with a **forged** banking check attached as a PDF file. This check intends to pay for needed work supplies. **Be aware: the threat actor's goal is to get you to deposit this check via your mobile banking app.**



This scam is convincing because the check is real; however, it includes forged routing and account numbers of another victim in the scam. The real risks come after depositing the forged check. This stage in the scam involves the threat actors corresponding with the student (still pretending to be RWU Payroll) to return any leftover money (via their mobile banking app) not used for office supplies. Once the initial victim becomes aware their money was fraudulently deposited to your account, their bank will request a return - **leaving the student out of the full check deposit and the additional "leftover money" returned to the threat actor's account for unused supplies.**

We expect this scam to morph over time. Today the scam centers around Summer internships and research projects but can easily change to other topics that retain the same tactics. Stay protected. **It's always best practice to validate these unsolicited requests by not responding directly; rather, forward the email back to the real professor using [RWU's online directory](#) to confirm its legitimacy.**

Sincerely,
IT Management

Don't take the bait! IT will never ask you for your username and password via email. Phishing e-mails attempt to deceive you into giving up private information in a response to a message or by leading you to a fraudulent web site.

For more tips about phishing, go to www.phishinginfo.org.

Follow Roger Williams University Information Technology on [Twitter](#) and [Facebook](#) for alerts, technology notifications, tips, and news.

This has been an official communication for Roger Williams University's Office of Information Technology. You are receiving this message because of your current relationship with Roger Williams University.

----- The All-Students Email Listserv is an informational Email List only. Please do not post or reply to this listserv.
----- The All-Students Email Listserv is an informational Email List only. Please do not post or reply to this listserv.