INFORMATION TECHNOLOGY
THE UNIVERSITY OF UTAH

ISO warns of stimulus payment scams

You're receiving this email because you're subscribed to UIT's public email list.

The U's Information Security Office (ISO) is urging students, faculty, and staff to remain cautious and alert to possible scams about the U.S. government's economic impact payments, often referred to as stimulus checks.

In recent weeks, the Internal Revenue Service (IRS) has reported a surge of scams against taxpayers that aim to steal their money or personal information, using the stimulus checks as leverage.

To better protect yourself, please follow these best practices from the Federal Trade Commission (FTC):

- Only use irs.gov/coronavirus to submit information to the IRS — and never in response to a call, text, or email.
- The IRS won't contact you by phone, email, text message, or social media with information about your stimulus payment, or to ask you for your Social Security number, bank account, or government benefits debit card account number. Anyone who does is a scammer phishing for your information.
- You don't have to pay to get your stimulus money.
- The IRS won't tell you to deposit your stimulus check then send money back because it paid you more than it owed you. That's a fake check scam.

If you have questions, your local IT support staff may be able to assist, or you may contact your respective help desk: UIT Help Desk (801-581-4000, option 1) or ITS Service Desk (801-587-6000).

Node 4 story idea? Email us: stratcomm@it.utah.edu

it.utah.edu

NotifyIT | **Follow us on Twitter** | **IT Services Status** | **IT Service Portal**