Appalachian’s Information Technology Services Security Team has been monitoring a recent widespread email scam related to fake job offers. These scams generally offer “too good to be true” conditions, such as high pay for minimal work, and ask for resumes to be sent via email verses a corporate application process. The goal of these fraudulent messages is to convince respondents to provide sensitive personal & financial information.

What To Do If You Have Received a Job Scam Email

- If you have received these emails forward them to phish@appstate.edu, then DELETE them
- If you have responded to them, we recommend that you end communication with these individuals immediately
- Do NOT provide them with any information

More information on spotting job scams can be found on the Federal Trade Commission site here: https://www.consumer.ftc.gov/articles/0243-job-scams

If you have questions or concerns specific to these messages, please contact ITS at the Help Desk at (828) 262-6266 or support@appstate.edu .

As always, feel free to send any suspicious emails to phish@appstate.edu.

Remember to Restart Your Computer! Here Are a Few Benefits...

- Critical patches have been placed, which requires a computer restart to take effect.
- Get into the habit of shutting down computers at the end of the day so that important patches & security updates can take effect on your computer once you log back in
- Flushes RAM, which is your computer’s main type of memory, thus flushing out random, unimportant & temporary data that could be bogging down your computer
- Increases performance speed