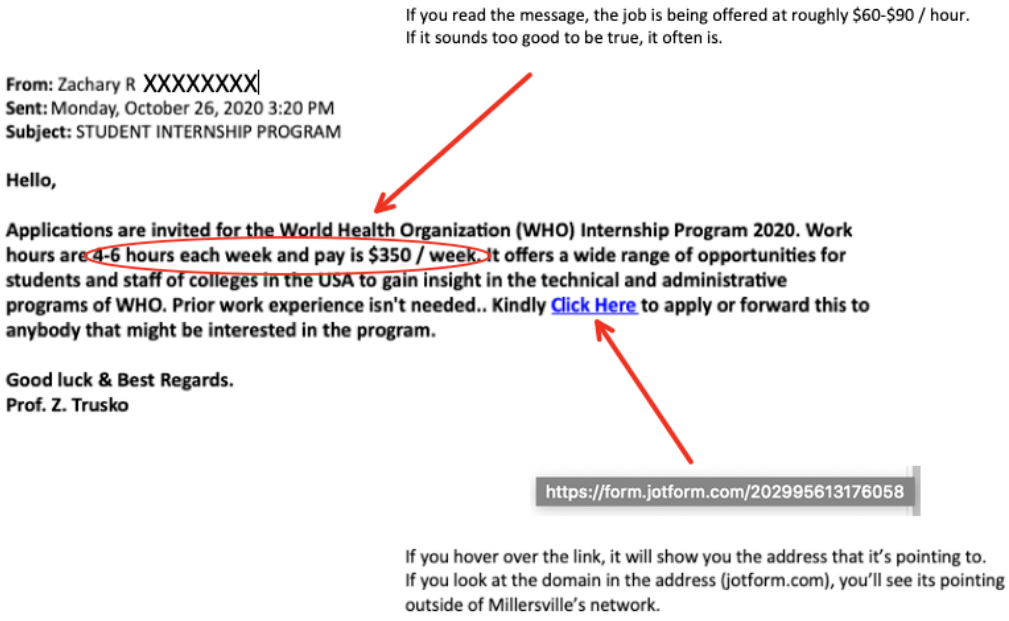
Increased Spam / Phishing Emails and Texts

Millersville IT has seen a dramatic increase in Phishing emails and texts the last few days. Phishing is the act in which nefarious individuals are attempting to trick our users into giving away personal and financial information. Often times, the sender of the email is an actual Millersville email account of a person who has had their credentials compromised. The attacker then sends out an email similar to the information below "offering" internships and jobs to other Millersville community members. Please review the example below and familiarize yourself with what to look for in the future.

If you did click on an email or text and lost funds please contact Millersville police at (717) 871-4357.

ACTUAL PHISHING EMAIL



Here are a few things to consider when you suspect you have received a suspicious email:

- **Don't reveal personal or financial information in an email**, and do not respond to email solicitations for this information. This includes following links sent in email.
- **Pay attention to the website's URL.** Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com versus .net).

- **Report it to the appropriate people**. If you receive a message you suspect as spam/phishing send it to the helpdesk or press the “Phish Alert” button in Outlook.