Watch out for the fake email job application scam

Published 3/28/2024 by Anna Dorbyk

The situation
The ITS team has seen an increase in phishing campaigns focused on job applications and recruitment. You may have received one of these scam emails.

Each of them is worded slightly different but generally say something to the effect of "Hiring NOW!!!" or "Home/On-Campus Job" with a PDF attached.

Here's what you have to know: Clicking on that attachment will generate a link, further prompting you to fill out a form with your personal information. It might all sound legit – it makes sense to fill out a form when applying for a job – but in this case you are sharing your personal information with scammers.

What is being done to protect your safety
ITS has implemented additional filters and security measures to detect and block these phishing emails and is closely monitoring the situation and responding quickly to any new threats.

What you need to do
Report any suspicious emails using the red 'Report Phish' button in Outlook. If anything looks off – report it – the ITS team would rather investigate a false alarm than miss a legitimate threat.

We also ask that you familiarize yourself with phishing email safety. Here are some of the basics:

- **Stay Alert**: Be cautious when receiving unsolicited emails related to job opportunities. Even if they seem genuine, exercise caution.
- **Verify Sender**: Always check the sender's email address. Be wary of external emails from free accounts (e.g., Gmail, Yahoo) that claim to be from a company.
- **Avoid Clicking Links**: Refrain from clicking on any links or attachments in emails unless you are certain of their legitimacy.
- **Beware of Attachments**: Be cautious when opening attachments, especially if they prompt you to enable macros or execute files.
- **QR Codes**: Avoid scanning QR codes from unknown sources, as they can lead to malicious websites.
- **Protect Personal Information**: Never share sensitive information (such as passwords, Social Security numbers, or financial details) via email.
- **Report Suspicious Emails**: If you receive an email that seems suspicious, report it immediately by using the 'Report Phish' button.

If you have any questions or concerns, please do not hesitate to contact ITS Service Desk, available 24-7.

tags : student-news