Research Phish

Recently the Penn community has been targeted by an email spoofing attack in which emails appear as if they are being sent from various Wharton Faculty. These emails look like legitimate correspondence from Wharton faculty, and target both current and incoming Wharton students. The emails offer financial compensation for participation in research projects. Requesting any sort of financial information, usernames and passwords, Social Security number, or any other personal information is typically an indicator of a mal-intended email. Students should be wary of any message that appears to be from a university employee requesting such information.

Anatomy of this Email Phish

This phish looked like it was sent by a Penn professor, but if you look closely at the reply address, it is not the professor’s actual email address. In addition, the student’s email address does not look accurate:

<table>
<thead>
<tr>
<th>from:</th>
<th><a href="mailto:professors.name@wharton.upenn.edu">professors.name@wharton.upenn.edu</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>reply-to:</td>
<td><a href="mailto:professors.name.wharton.upenn.edu@gmail.com">professors.name.wharton.upenn.edu@gmail.com</a></td>
</tr>
<tr>
<td>to:</td>
<td><a href="mailto:student.name@wheels-student.org">student.name@wheels-student.org</a></td>
</tr>
</tbody>
</table>

The introductory text seems fairly believable:

This is an invitation to work remotely from home in a multidisciplinary research project as a temporary research aide collecting data online and earn $250 weekly. This is an adaptable job that requires little to no prior experience. Indicate interest by providing the required information below and I will send you a follow up email with details.

Full Name:
Cell #:
Alternate email:

In the case of this phish, followup emails -- several of them -- requested more directly personal information, all of which can be used to steal identity or personal funds. Poor grammar also is a clue that it is a phish. Here's one example:

Send in your resume for review and respond to the few questions below
- Current Address:
- Age:
- Bank Name (this is so your paycheck can be processed accordingly and as at when due)

- I'll appreciate you keeping me in the loop while performing your task and prompt response to our text/email correspondence is expected so I know you are on the job.

Regards

General Phishing Advice

Unfortunately, anyone with an email account may be susceptible to receiving deceitful messages that seem to be from a "friendly" sender. Typically, these messages will attempt to get users to share personal information by clicking on a fake link, or by having you send the sensitive information directly. For more information on phishing and scams, see our Guide to Spam and Phishing.

Wharton staff and faculty will never try to obtain your password, or any other sort of personal or private information via email. If you do receive an email requesting this sort of information, feel free to ignore it, delete it, or forward it to your support representative.