

Be Alert for Computer Support Scams

changed 01/24/2013 - 5:56pm

The Security Office in ITS-Network services has become aware of multiple attempts to conduct social engineering attacks against UNI employees. The attack originates as an off-campus phone call purportedly from a technical support person and they attempt to instruct the user to install malicious software on the computer claiming that the software is needed to fix the computer. This software can then be used to steal information stored on the computer, to conduct further attacks, or to participate in other illegal activities. Similar attacks will attempt to get users to disclose their passwords.

If you are uncertain of the legitimacy of any call from IT staff, politely inform them of your concerns, hang up, and call your usual support number directly. Further, never provide your passwords to anyone. UNI will not ask for your passwords. If asked to provide your password, end the conversation immediately.

Please report any instances of such attacks by emailing security@uni.edu [1].

Source URL: <http://www.uni.edu/its/news/2013/01/4/be-alert-computer-support-scams>

Links:

[1] <mailto:security@uni.edu>