

From: [Eldayrie, Elias G](#)
To: [CIO-All-Students](#)
Subject: Phishing Awareness
Date: Friday, August 17, 2018 10:27:00 AM
Attachments: [image003.png](#)

Students:

Welcome, or welcome back to UF! I know this is an extremely busy week but I have an important message for all members of Gator Nation.

Identity theft crimes are so common that we read about a new breach daily on our social media feeds. I'd like to ask for your help in combatting phishing and identity theft crimes at UF. Phishing is when a cybercriminal attempts to steal personal information through social engineering. Often, the email is made to look like it comes from a familiar organization, like the UF Computing Help Desk or the university's president, but contains a link that takes you to a website set up to steal log-in credentials and personal information. GatorLink password credentials have been stolen and we've had students give up personal information (including their address and bank account number) via phishing emails. To help you make more informed decisions, please remember:

1. NO ONE SHOULD EVER ASK FOR YOUR GATORLINK PASSWORD. YOU SHOULD NEVER PROVIDE IT TO ANYONE! Not by email, phone, in person, or by any other means.
2. Before clicking on a link embedded in an email, place the mouse pointer over the link and inspect the web address the link goes to. If you are suspicious of the web address...do not click.

Students who think they have clicked on a phishing link should immediately change their GatorLink password. Assistance changing GatorLink passwords is available 24/7 from the UF Computing Help Desk (352-392-HELP/4357). More information on phishing awareness and staying safe online is available for you at <https://security.ufl.edu/welcome/>.

Have a great semester and Go Gators!



Elias G. Eldayrie
Vice President and CIO

