SOUTHERN UNIVERSITY
AND AGRICULTURAL & MECHANICAL COLLEGE
Information Technology

Division of Information Technology
Suite 140, J. B. Moore Hall
P. O. Box 12891
Baton Rouge, Louisiana 70813

Voice: (225) 771-3935
FAX: (225) 771-2883
http://www.subr.edu

May 2, 2019

ATTENTION SOUTHERN UNIVERSITY SYSTEM COMMUNITY

CYBERCRIMINALS ARE USING SOCIAL ENGINEERING TECHNIQUES TO CONDUCT PAYROLL DIVERSION

Attention SUS Community! Institutions of Higher Education are seeing increasing phishing and spear-phishing emails targeting employees' payroll. These emails subject varies in nature but designed to capture an employee's Banner login credentials. Once the cybercriminal has obtained an employee's credentials, the credentials can be used to change direct deposit information, redirecting the payroll funds to an account controlled by the cybercriminal, which is often a prepaid card.

Another variant of the **Payroll Diversion** scheme is a spear-phishing email directed at specific HR and Payroll personnel. Often these emails are disguised as an innocent request from a University employee asking for their payroll/benefits information be changed to a new account.

The Division of Information Technology **(DoIT)** is calling your heightened attention to beware of these emails and NOT fall prey to these scams. In a recent report released by the Federal Bureau of Investigations **(FBI)** Internet Crime Complaint Center **(IC3),** more than **$100M** was lost by victims in 2018. If you would like more detailed information on this please go to the following link and read the complete FBI Internet Crime Report and analysis.

https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf

We are providing these reminders to members of the Southern University:

1. Be suspicious of communications from emails that come from an external email address that is not a work email, for example: **Name <homemoble@officefacx.com>** or from **ADMIN HR (PAYROLL)**. Review the sending email address closely to see whether it is a Southern University Address.
2. Check with the apparent sender by phone call, chat, or in-person if you are at all unsure, or send a separate email to the person's usual email address. **Do not reply to the request itself.**
3. Ignore any request to change banking information by email. All banking information should be done through the proper procedure of the University and not via email. **Anyone who made this request is not following University procedures.**
4. Report email impersonating people to DoIT unit on your respective campuses.
5. Ask DoIT if you suspect an email is most likely a feeler message so that you could respond and get further email instructions.

We filter hundreds of thousands of phishing/spam emails on daily basis but the ultimate responsibility is yours. Please take all the precautions very seriously. Thank you.