From:	Eichler, Emily J. on behalf of Rounds, Mike
To:	KU Lawrence All Staff, Faculty and Affiliates; KU Graduate Teaching Assistants; KU Graduate Research Assistants; KU Graduate Assistants
Subject:	ALERT: Be aware of fraudulent unemployment claims
Date:	Wednesday, September 16, 2020 10:12:51 AM

KU Employees,

In June we told you that criminals are taking advantage of the COVID-19 pandemic and economic uncertainty by filing fraudulent unemployment claims using stolen personal information. This activity is widespread and, like most universities and many other organizations, employees at KU have been targeted.

If you receive an unemployment notice that you were not aware of or didn't initiate, please contact KU Human Resource Management at hrdept@ku.edu and Employee Relations staff will alert the necessary State of Kansas personnel to stop the benefit**.**

How does this happen?

It appears that criminals are using personal information that was posted to the dark web after previous nationwide data breaches. KU IT Security has found no evidence to indicate a breach of our campus systems. KU Information Technology has extensive security measures in place to protect personal and confidential information, including encrypting data stored in our systems and when data is transmitted. And, Duo multifactor authentication is required when logging into HR/Pay. The fact that you may know multiple colleagues who have been targeted shows how widespread fraudulent unemployment activity is now.

What should you do?

If you receive an unemployment notice that you believe is fraudulent, contact hrdept@ku.edu immediately. HRM will work with you and the Kansas Department of Labor to resolve the issues within state of Kansas systems.

In addition to reporting the fraudulent unemployment notice to hrdept@ku.edu, you should consider other steps to monitor and/or secure your credit report and prevent further identity theft. The Federal Trade Commission provides information for getting started. These steps can include placing a fraud alert on accounts and freezing your credit report.

How can you protect yourself?

Even if you have not been targeted in unemployment or other fraudulent activity, the FTC recommends steps to protect yourself from identity theft.

In addition to the FTC recommendations, KU Chief Information Security Officer Julie Fugett and I remind you to be on guard for phishing and other cyber-attacks. Criminals are exploiting

the uncertainty and fear surrounding the COVID-19 pandemic and you can protect yourself by:

- **Being vigilant:** If you receive a notification you didn't expect — from the university, a government agency, a bank, etc. — contact the organization immediately using a phone number or email listed on their website. Don't reply or use contact information in the email, as it may be fake. If you get suspicious emails to your KU address, send them to abuse@ku.edu. Contact KU IT Customer Service center at 785-864-8080 or itcsc@ku.edu if you have security concerns related to KU systems or data.
- **Being proactive:** Change passwords for your online accounts on a regular basis, or if you get unusual notifications or see suspicious activity. Use complex passwords. Use multifactor authentication whenever possible on personal accounts. KU requires Duo multifactor authentication for access to campus systems.

The National Cybersecurity Alliance provides additional information and tips for protecting yourself.

Contact Human Resource Management at hrdept@ku.edu if you receive notification of unemployment benefits you did not file for through the Kansas Department of Labor. To learn more about the fraudulent claims in Kansas, read the notice from the Kansas Office of Information Technology services. If you are interested in learning more, the Kansas Department of Labor website has more information about unemployment benefits and fraudulent claims.

Respectfully,

Mike Rounds
Vice Provost for Operations