

From: [KU Information Technology](#)
To: [KU Information Technology](#)
Subject: Protecting against unemployment fraud
Date: Monday, October 26, 2020 12:20:06 PM
Attachments: [KDOL State Employee UI Fraud Letter 10.20.20.pdf](#)

KU Employees,

Unemployment fraud is a continuing concern across the country. Criminals are using stolen personal information of employees from all types of organizations — higher ed, companies and government — to file fraudulent unemployment claims.

The attached letter from the Kansas Department of Labor outlines the scope of the problem: 100,000 fraudulent claims in Kansas alone at a cost of \$8 billion to date. The letter provides additional important details for state employees, including how to report a fraudulent claim. (Affiliate employees, please check with your Human Resources staff for guidance.)

[Where do criminals obtain personal information?](#)

It appears criminals are using personal information — names, addresses, social security numbers — from previous nationwide data breaches. For example, one of the three major credit agencies reported a massive data breach in 2017. KU IT Security has found no evidence to indicate a breach of our campus systems.

KU Information Technology and KU Human Resource Management have heard concerns from KU employees that salary or other personal information has been stolen from the university. Employment data for state employees, including salary information, is available to the public, which makes our information more accessible. Criminals may be harvesting information through these public sites and mapping them with other data they have collected separately.

[How does KU IT protect personal information?](#)

KU Information Technology has extensive security measures in place to prevent and detect cyber-attacks. KU IT also has systems and procedures to protect personal and confidential information, including encrypting data stored in our systems and when data is transmitted. You help us protect your information by using Duo multifactor authentication when logging into HR/Pay and other KU systems.

[What should you do?](#)

If you receive a fraudulent unemployment claim from KDOL, please take action immediately by reporting it at www.ReportFraud.ks.gov. We also ask that you notify KU Human Resource Management at hrdept@ku.edu. Affiliate employees should check with their Human Resources staff for guidance.

In addition, 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, 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 the IT Security Office at itsec@ku.edu if you have questions or concerns about the security of our systems or the protection of your personal information. Contact Human Resource Management at hrdept@ku.edu if you have questions or concerns about fraudulent unemployment claims.

Respectfully,

Mary Walsh
Chief Information Officer

Mike Rounds
Vice Provost for Operations