700 SW Jackson Street
Suite 803
Topeka, KS 66603

Kansas
Department of Credit Unions

Phone: (785) 296-3021
Fax: (785) 296-6830
kdcu.office@ks.gov
www.kdcu.ks.gov

Jerel Wright, Administrator

Laura Kelly, Governor

DATE: **July 13, 2020**

BULLETIN: **2020-KDCU-CUB-14**

TO: **Kansas Chartered Credit Unions**

SUBJECT: **Cybersecurity**

CYBERSECURITY

With the COVID-19 pandemic came an increase in employees working from home which, of course, led to increased scrutiny on cybersecurity. Does your credit union remain in good "cybershape"? Are you confident appropriate safeguards are in place amongst your workforce? Don't forget your members – how is the cyberhealth of your online and mobile banking experience? Cybersecurity remains a constant challenge for credit union staff.

On July 7, 2020, the Financial Crimes Enforcement Network (FinCEN) issued an advisory on imposter scams and money mule schemes related to COVID-19. The basic methodology for imposter scams is contacting a target under false pretenses and requesting funds or information. This generally comes in the form of an email which is used to infect the user's computer with malware or ransomware. The scammer(s) may impersonate legitimate charities or the government. Email phishing schemes could also involve stimulus payments issued pursuant to the CARES Act. "Money mules" are unwitting individuals recruited to assist in financial criminal enterprises, e.g., unemployment insurance. These situations can be stopped by credit unions who "know their members" and their normal financial transaction activity. Financial institutions are encouraged to perform inquiries and investigations where appropriate.

The Federal Bureau of Investigation (FBI) issued a Public Service Announcement on June 10, 2020, warning how increased use of mobile banking applications could lead to exploitation. Studies indicate a 50% surge in mobile banking since the beginning of 2020. With the social distancing mandate, this number may continue to rise. Have you checked the security on your mobile app platform? If you become aware of malicious activity, complaints may be filed with the FBI's Internet Crime Complaint Center (IC3). A FBI Flash Alert, with technical details, was issued on June 22, 2020.

Previously, the NCUA issued Risk Alert No. 20-RISK-01 addressing cybersecurity considerations for remote work. Credit union management was reminded that employees working remotely should adhere to information security and privacy-related policies and procedures. The policies and procedures should address the prevention of security incidents and include provisions for responding to incidents that do occur. Additional institution-level controls should be considered and addressed in your risk assessment.

In addition to NCUA Cybersecurity Resources, the Federal Financial Institutions Examination Council (FFIEC) provides multiple resources on their website, including the Cybersecurity Assessment Tool. FinCEN provides guidance on the reporting of cyber-events through Suspicious Activity Reports.

NOTE: In accordance with Governor Laura Kelly's Executive Orders and the Ad Astra Plan, KDCU Administrator Jerel Wright continues to review the feasibility of resuming the on-site examination program. This is being done in coordination with the NCUA.