

DATE: December 13, 2021
BULLETIN: 2021-KDCU-CUB-25
TO: Kansas Chartered Credit Unions
SUBJECT: Ransomware

RANSOMWARE

On November 8, 2021, the Financial Crimes Enforcement Network (FinCEN) issued [Advisory FIN-2021-A0004](#), entitled “Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments.” This advisory updates and replaces the October 1, 2020, advisory. In recent months, ransomware attacks have increased and financial institutions, as part of the critical infrastructure, are not immune.

On the same day, the Board of Governors of the Federal Reserve System issued their semi-annual [Financial Stability Report](#). Included in this report is a section on “Cyber Risk and Financial Stability” (pp. 70-72).

Ransomware attacks are a growing concern for financial institutions because of their role in the collection of ransom payments. Sample schemes provided by FinCEN include the following:

- **Extortion:** “Double extortion schemes” are becoming more prevalent. These involve removing sensitive data, encrypting it and demanding ransom. In many instances, the system breach is used to target additional parties. Third parties provide the attacker with additional leverage. Does your credit union use third party vendors?
- **Use of cryptocurrency:** Many cybercriminals require ransom to be paid in convertible virtual currency (CVC), *e.g.*, bitcoin. However, victims may now be asked to pay in “anonymity-enhanced” CVC which can reduce the transparency of the transaction. This choice may even earn the victim a discount! A keyword search of your membership transactions may uncover a number of cryptocurrency transactions, *e.g.*, Coinbase. The majority are not illegal, but wouldn’t it be interesting to know how active your members are in this area?
- **“Fileless Ransomware”:** This is a sophisticated tool, challenging to detect, which can cause the malicious code to be written to the computer’s memory rather than a file on a hard drive. This allows cybercriminals to circumvent off-the-shelf antivirus and malware defenses. How good is your cybersecurity?

If you sense a cyber theme to the bulletins over the past year, you would be accurate. Cybersecurity has increasingly become more important to financial institutions and, of course, is always at the top of the NCUA’s priority list. In today’s ever-connected, online-dependent world, it is vital Kansas credit unions understand the importance of cybersecurity and maintaining their cyber hygiene. More importantly, do not think it cannot happen to you.

NOTE: In accordance with Governor Laura Kelly’s [guidance](#), KDCU Administrator [Vickie Hurt](#) continues to review the feasibility of resuming the on-site examination program. This is being done in coordination with the NCUA.