July 23, 2026

Be Alert for Phishing Email Targeting Vermont Municipalities

Current as of: 9/12/2026

The Vermont Intelligence Center (VIC) has let us know of a phishing campaign that was reported to the VIC by a Vermont municipality.

In this phishing campaign, cyber threat actors were able to compromise the email addresses of organizations in Vermont and use those legitimate email addresses to send phishing emails to a municipality in the state. The phishing emails came in the form of encrypted Microsoft emails in which the recipient must log in to an encrypted portal to view the message. The emails then contain a link that in previously observed cases resolved either to a 404-error page or a webpage with a CAPTCHA prompt. The CAPTCHA verification could potentially indicate a ClickFix attack, which uses CAPTCHA verifications as a vector for compromise.

The link that has been observed being distributed in these emails is: hxxps://sabujbanglatv[.]com/ms365authsharpointpathway/sharpoint-proofpoint-verified.html

Additionally, among the legitimate Vermont-based email domains used to send these phishing emails so far are:

"Ruraledge[.]org" and "vtlegalaid[.]org"

Organizations in the state should be vigilant of unprompted encrypted emails being received from outside entities. **If an unprompted email of this nature is received, it is recommended to reach out directly to the entity or individual that sent it to confirm if it is legitimate.** If these emails are identified and believed or determined to be illegitimate, standard practices should be followed to report it to the organization's IT department. It is also requested that these cases be reported to the VIC by reaching out directly to the VIC's Cyber Analyst at ryan.mcliverty@vermont.gov. The VIC is trying to assess the scale of this phishing campaign and determine similarities among the target organizations.