

CrowdStrike Compromised Password Information

Beginning October 20th, 2025, students, faculty, and staff will receive automated notifications from CrowdStrike informing them that their password has been detected as compromised.

This message originating from falcon@crowdstrike.com is legitimate and does not indicate any malicious activity. Recipients of these messages should be aware that a password change must be completed prior to 5:00 PM the day of receipt. If this is not completed before that time, a password change will be **required** at their next login.

This process is executed daily, with regular updates to the compromised password databases. As a result, passwords previously considered secure may subsequently be flagged as compromised and require resetting.

All students, faculty, and staff passwords are continually monitored under this protocol to ensure A-State resources remain secure.

Below is an example of the email users will receive if their password is flagged as compromised:

Arkansas State University - Password reset request

F

falcon@crowdstrike.com

To:

Reply

Reply all

Forward

...

Wed 10/8/2025 1:30 PM

This Message Is From an External Sender

This message came from outside your organization. Please be careful.



Dear User name,

Our security team has identified that your current password has been found in known data breaches or compromised password lists. To protect your account, a password reset request will be made for your A-State account at 5:00 PM today. If your password is not updated before then, you will be required to change your password on your next login.

Password reset steps can be found in this Knowledge Base article: <https://kb.astate.edu/books/microsoft-password-reset/page/microsoft-change-password-when-already-signed-in>

This new password must meet the following minimum criteria:

Minimum Passphrase Length Requirement: 15 characters

Complexity: Passphrases must include at least one uppercase letter, one lowercase letter, one number, and one special character. It is strongly encouraged to avoid repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd').

Thank you for your prompt attention to this critical security matter.

Thanks,

ITS Security Team
security@AState.edu

Copyright © 2025 CrowdStrike, Inc. All rights reserved.

Tips for identifying these emails as non-malicious:

1. The sender address is falcon@crowdstrike.com
2. This message is marked as “from an external sender” due to CrowdStrike not being an internal resource.
3. This message requires no action from the recipient. There are **no** forms, **no** requests for a reply, and **no** directions to reply from an email address not associated with A-State.
4. No user information is requested. As this is from a legitimate source, any necessary information is already available to the ITS Security Team.

If you ever doubt the legitimacy of an email or communication, reports can be submitted to security@astate.edu for review.

Revision #4

Created 2025-10-08 18:02:19 UTC by Kelsie McDole

Updated 2025-10-09 14:18:49 UTC by Kelsie McDole