## Fraudster Wave Strikes Again 5/31/2024

Yesterday evening, May 30, there was another wave of a fraudster(s) impersonating Denison State Bank in texts to some local people, saying that DSB discovered unusual transaction activity on their bank account and inviting them to click a link to fix the problem. This link took them to a non-DSB site where they were prompted to reveal identifying information, such as full DSBconnect login credentials, which can allow the fraudster to login as the victim and schedule outbound funds transfers. The speed of transfer depends on which banking tool the fraudster uses: debit card, P2P, Bill Pay, ACH.

If you received such a text and took these actions, you should login to your DSBconnect, if possible, and click Profile and change your username, password, security answers, and delete any unknown phone number that got set up in Devices. If unable to login, the fraudster already changed the credentials – respond back here if that happened. If you find any unauthorized transaction posting, report it to us.

This was not a breach into our banking systems. We cannot prevent fraudsters from impersonating us. Mobile phone numbers can be obtained in the illegal underworld. These texts are being sent to DSB account holders and non-DSB account holders alike. Other industries, besides banking, are also victims of illegal misuse of name and brand identity.

Remember:

- The only automated texts that our systems send out are those that account holders set up themselves in their DSBconnect > Manage Alerts. You can see which texts our system sends to you there in Manage Alerts instead of relying on what shows up in your text inbox. There are times that our bank employees will text or email bank customers, but those are normally more narrative about a known situation and not an account/transaction alert.

- The only place where DSB prompts for entry of username and password is at the login screen for DSBconnect. We never ask for that anywhere else.

- We never ask for full debit card number, PIN, expiration date and 3-digit security code in that combination.

- The only way a fraudster can login to DSBconnect as you is to know your username, password, security answers, and have a multi-factor authentication sent to his own device. We have found the only way for a fraudster to obtain those is by fooling the account holder to reveal that information in a spoof communication.

- Fraudsters tend to be active during non-banking hours, weekends and holidays.

- Please take time at the below links to learn how DSB protects your banking identity and information through fraud prevention and recovery:

DSB Fraud Guide:
https://www.dsbks.com/home/fiFiles/static/documents/DSB%20and%20Customers%20Fight%20Bank%20Fraud%202022.pdf

*(continued next page)*

What Official DSB Communications Look Like:
https://www.dsbks.com/home/fiFiles/static/documents/DSBFraudImpersonatorsLegitCommunications.pdf

Multi-Factor Authentication:
https://www.dsbks.com/home/fiFiles/static/documents/OOBA%20MFA%20Dec%202023.pdf

DSBconnect Alerts:
https://www.dsbks.com/home/dsbconnect/mobile-apps/dsbconnect_text

If any questions or concerns, respond back here. Whenever in doubt, feel free to call us during banking hours: 785-364-3131.

**Denison State Bank**
**Digital Banking**