During these uncertain times, NVE is here for you and will continue to provide you with the high-quality service you are accustomed to. In an effort to do this, we find it important to make you aware of security risks that may arise. Early indications show that fraudsters may be increasing Phishing, Online Fraud, Account Takeover and Identity Theft attacks to exploit the current COVID-19 pandemic. This includes impersonating Banks, Health Groups and Federal Government Agencies.

Below are helpful tips to keep your Identity and Finances secure:

- As with any electronic message, please use caution when responding to incoming inquiries as fraudsters have the ability to 'spoof' or change the originating telephone, text or email address.
- Check your account daily through online banking, mobile banking or telephone banking for any unauthorized transactions and report them to us immediately.
- Use complex passwords. We urge customers to avoid using browser settings to automatically store passwords.
- If NVE is contacting you regarding recent transactions on your debit card, we will never ask for your PIN, Expiration Date or the 3-digit security code located on the back of your card. We will only require your zip code.
- NVE Bank will never contact you via text, email or phone asking for personal or bank account information.

Your online security has always been NVE Bank's top priority. If you believe you may have been a victim of any of these online attacks and need assistance with your account, please call your local NVE Bank branch.