It is important to First National Bank of Middle Tennessee (FNBMT) to keep you updated and we understand your inboxes are being consumed with "Corona Content" so we will keep this short.

When reaching out to you we will not ask for personal or financial information or access codes through email, text, unsolicited calls.

Fraud risk is on the rise- As email phishing attempts are likely to rise using IRS or Corona call to actions in email subject lines. Continue to stress caution when opening emails from those parties or you have no affiliation with.

a. *Payment Fraud*- With employees working remotely, stress verbal confirmation for payments and where you can implement dual authorization.
b. *Mail*- With many working out of the office, mail is sitting idle and at risk. **If you do not use Positive Pay to mitigate check fraud, you should STRONGLY consider adding it.** Please contact us at Heather Steele or Ryan Crouch at 931-473-4402, or by email at hsteele@fnbmt.com or rcrouch@fnbmt.com, if you fall in this group.
c. *Track account activity*- Between remote working, idle mail and other risks, be diligent in actively checking your account activity multiple times a day.

Fraudulent requests for wire transfers typically come by email. Security tips to help you stop potentially fraudulent requests for wire transfers.

1. **Verbal Confirmation**
   Verbally confirm that the request to initiate the wire is from an authorized vendor or person within the company.
2. **Verify Changes**
   Anytime you receive new wire instructions or a change to existing wire instructions verbally verify with your wire transfer vendor.
3. **Investigate Unique Requests**
   If you receive a request for a payment that is out of your ordinary payment arrangement, confirm by phone with your vendor.
4. **Double Check Email Addresses**
   A common trick is to slightly modify an email address. For example, john.smith@abc.com might be changed to jon.smith@abc.com
5. **FWD Instead of Reply**
   Rather than reply to an email, forward the email to the address that you have on file.
6. **Establish Dual Controls**
   This could mean having one FNBMT user who initiates the wires and another FNBMT user who approves the wires.
7. **Be Alert**
   Be on alert for fraud anytime the wire transfer instructions include tight deadlines or pressure you to act quickly.
8. **Be Suspicious of Confidentiality**
   Whenever wire transfer instructions specify keeping the transaction a secret – verbally verify with an executive or the person requesting the transaction.

The best defenses against wire fraud include rock-solid internal procedures and training team members to recognize the signs of suspicious activity within the company.

If you have questions, please contact:

Heather Steele
SVP, Treasury Management Sales Officer

(O) 615-956-0273
hsteele@fnbmt.com

Ryan Crouch
Banking Officer
Treasury Management Implementation Specialist
(O) 931-474-4989
rcrouch@fnbmt.com