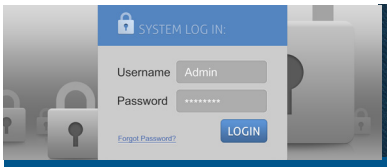

ACCESS NATIONAL BANK
The Difference is Access.

Middleburg Bank
A Division of Access National Bank

IMPORTANT NOTICE
BUSINESS EMAIL COMPROMISE SCAM

The banking industry has seen an increase in wire fraud. A scam that is increasing in volume and sophistication is called Business Email Compromise (BEC), also known as C-suite email fraud or CEO email fraud.

In short, criminals are hacking into email systems of businesses. Once inside the email systems, criminals monitor emails to identify internal/external senders and recipients who have the ability to act on and/or authorize wire transfers. The criminals then intercept and inject wire transfer email instructions posing as someone authorized to approve payment orders, like the CEO, CFO or other executive officers of the company.

The email request may be forwarded to a person within the company who initiates business wire requests to the Bank. The employee believes the email to be a legitimate request from the company's c-suite or other authorized employee and initiates the wire. When the Bank receives the wire transfer request from the customer, using established verification procedures (User ID, Password, Callbacks), the Bank processes the wire as usual.

HOW DO I PROTECT MY BUSINESS?

It is best to establish internal controls to ensure your employees do not respond to fraudulent emails. The following are best practices to consider:

- **Execute call-back verifications for any financial transaction requested by email or text message, regardless if the email is from your company's executives, a trusted employee or a vendor.**
- Require internal dual control approvals for all transactions requesting a wire transfer.
- Set limits for employees that have wire transfer authority.
- Install and maintain anti-virus, anti-spyware and anti-malware software on all business computers.
- Conduct regular security awareness training with employees.
- Advise all employees to exercise extreme caution when asked to divulge account information or banking credentials.
- Don't deviate from existing procedures. Any exceptions should be scrutinized.
- Be careful when posting financial and personnel information to social media and company websites. Be careful not to post or have employees divulge exact vacation dates of executives. BEC fraud often occurs when an executive is out of the office.

WHAT RED FLAGS MAY ALERT ME TO A PHISHING EMAIL THAT COULD LEAD TO A COMPROMISE?

- **Did you read and re-read the entire email?** The subject line may look fine, but if you do not read the body of the email, you may make a big mistake. Does the request or instruction make sense to you? If the email is coming from someone you know, would he or she write an email like this one? Does this sound like something he or she would say or do?
- **Does the email address look legitimate?** Look **closely** for misspellings, dashes, dots or anything else that should not be there. Is the format correct? For example: sally.smith@abccompany.com vs. ssmith@abccompany.com vs. sallie.smith@abccompany.co
- **Are you the right person to receive the email?** Would **you** normally receive this type of request by email or otherwise? If you do recognize the sender, has the sender dealt directly with you in the past? If not, how did the sender get your email?
- Are there **misspellings** in the email?
- Is there incorrect or **improper grammar**?
- Does the sender **use the word, "kindly**?"
- Is there a **link included in the email**, sometimes masked by a button that may read, "Click Here" to enter your information? (or something similar)
- Is there an attachment, but nothing or very little written in the body of the email?
  For example: "Take a look at this!"
- Is the email requiring **secrecy or urgency in action**?
- Does it include **a threat**? (i.e. to cut off service, close an account, stop a shipment, etc.)
- Does the **web address match the business name of the sender**?
  For example: The email was sent from the ABC Company, yet the address is www.systems.uk.
- Does the sender **ask for non-public personal or bank proprietary information**?
- Does the sender **ask for your computer credentials; such as, user name, password, etc.**?
- Does the wording in the email state that they are asking you for this information **to help you prevent fraud**?
- Is this **email from someone you don't know**? (i.e. a bank where you do not have an account, a lottery you didn't enter, etc.)

WHAT DO I DO IF I SUSPECT A COMPROMISE?

In the event of a compromise, notify the Bank and law enforcement, as soon as you detect the fraud. **Early notification is critical**, especially if funds were wired. The longer it takes to report the fraud, the less chance of funds recovery.

No business is immune to this type of fraud. Business Email Compromise schemes are becoming an increasing threat to companies worldwide. We highly recommend taking preventative measures, utilizing technology and internal controls to protect your assets.

Additional information can be found through a Public Service Announcement from the FBI, located at: https://www.ic3.gov/media/2017/170504.aspx.