Phishing Awareness for ACH and Cash Management Users

St. Johns Bank wants you to be aware of “phishing” scams that are circulating in hopes that you will not become a victim. Many people think that consumers are the only targets for identity theft, but businesses are also a favorite target for scam artists, because they have an online banking account that will allow the business to originate ACH entries and/or wire transfer entries.

“Phishing” is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. Another variance of this scam is “smishing,” which is a cell phone text message asking for private information, and “vishing,” which is making a caller ID window appear to be a legitimate business, so the person answering the phone will be more open to providing private information.

Here are some tips to avoid being a victim of these “phishing” scams:

- St. Johns Bank will never send an e-mail requesting you to click on a link to sign in to your account or to call a phone number to provide private information.
- Whenever you sign in to your NetConnect Cash Management account, always use your normal process (e.g., a Favorites link or our homepage link). Do not use a link sent in an e-mail.
- If you receive a suspicious e-mail or phone call, do not hesitate to call us to ask us about it. We do not mind looking into the matter for you.
- If you call us, you should use our main phone numbers (314) 428-1000, (314) 428-1059, or (636) 939-3495. Do not use a phone number sent to you in an e-mail or left on an answering machine.
- If we call you and you want to be sure that the phone call is legitimate, ask us for our name and tell us that you will need to call us back (using one of our main phone numbers). We do not mind if you take this extra step to protect your information.
- Be suspicious of unanticipated e-mails that request you to open an attachment. These may be actually installing a keystroke logging virus on your computer.

We hope that you will find this information helpful. If you have any questions or concerns, please do not hesitate to contact us at (314) 428-1059, Extension 3472.