

Important Information About Internet Fraud

“Phishing” is an online scam involving fraudulent email messages asking for confidential information such as passwords or account numbers. These emails, which are disguised to look like requests from legitimate companies, can be very convincing. They are intended to steal your personal information and use that information to access your accounts. NorthStar Financial Services Group, LLC (“NorthStar”) will not send you an email requesting personal information, unless you initiated correspondence.

Typical Phishing Messages

A Typical phishing message might identify a “problem” with a recipient’s account. There is often a sense of urgency-an account may be closed for example-if the requested information is not provided.

What to do

Phishing emails often instruct recipients to click on a link, which will direct them to an official looking Web page. Never reveal personal data within an email or when visiting a website that you were brought to by a link in an email. If you are suspicious of an email, go directly to the website via an official URL instead.

NorthStar’s email policy:

As noted, we will not send you an email requesting personal information.

We send emails if:

- You requested to receive document updates electronically
- You requested email delivery of information as a follow-up to a specific telephone call
- You requested non-personal, non-account-related information that can safely be responded to via email
- You supplied us with an email address and have not specifically indicated that you do not want marketing materials

When in doubt, contact us: If you suspect that you’ve been sent a fraudulent email, please forward it to us immediately at phishing@nstar-financial.com. Please note: This email address is exclusively for messages related to suspected email fraud. Please do not use this email address to send us general questions about your account(s).