

**Please be advised that there are variations of a “Phishing” email circulating. These emails *are not* from FirstBank.**

**Anyone who receives any of these emails is advised to delete them without responding or clicking on any links within the email. If you have any questions, you can contact your local FirstBank branch or FirstBank’s Electronic Banking Department at 1-800-413-4211.**

*First sample of fraudulent email:*

**From:** First Bank [mailto:securityalerts@firstonline.com]  
**Sent:** Sunday, December 21, 2008 11:48 AM  
**To:** undisclosed-recipients:  
**Subject:** Update your profile



---

**Dear Customer,**

First Bank is serious about safeguarding personal information online. We follow rigorous security procedures to protect your information and transactions against unauthorized access. Our entire system was developed from the ground up to retain the confidentiality of our customer’s information. Our customer’s information is of utmost importance and we maintain procedural safeguards that comply with federal standards to protect personal information.

Recently, our online security team discovered that your online banking access information needs to be updated. This is a regular measure you should take to prevent fraudulent and unauthorized activities from your accounts.

We therefore require 3-5 minutes of your time to update your online banking access information. Doing this will forestall future problems when using First Bank online banking service.

Please note that failure to update your information will lead to the suspension of your access to online banking. We sincerely regret any inconveniences.

**[Update your online banking information](#)**

Best Wishes,

**Brenda O. Jackson**  
**Head of Online Banking**  
**First Bank**

---

Because your reply will not be transmitted via secure e-mail, the e-mail address that generated this alert will not accept replies. If you would like to contact First Bank with questions or comments, please sign in to online banking and visit the customer service section.

©2008 First Bank. All rights reserved.

*Second sample of fraudulent email:*



---

**Dear Customer,**

**First Bank** has been under severe spamming and phishing attacks in the last few weeks. Consequently, we are upgrading our servers to withstand these drastic surge of cyber attacks. We will also be introducing an additional security layer in our online banking. Due to these upgrades, you may experience interruptions while using **First Bank** online banking. To prevent this, update your online banking profile by clicking the link below:

**<https://www.firstbankonline.com/onlinebanking/update/>**

**NOTE:** For security reasons, you will need to provide your User ID, Password. You will also be required to enter your correct challenge questions and answers. We appreciate your understanding and apologize for any inconvenience.

**CAROLINE S. JOHNSON**  
**Head of Online Banking**

---

As outlined in our User Agreement, **First Bank** will periodically send you information about site changes and enhancements. Visit our Privacy Policy and User Agreement if you have any questions.  
Copyright© 2008 - First Bank. All rights reserved

*Third sample of fraudulent email:*



---

**Dear Customer,**

**First Bank is carrying out a scheduled yearly online banking systems update. Consequently, in the next couple of weeks, you may notice some interruptions when using online banking. To experience a smoother online banking, update your information with us by clicking on the link below.**

**<https://www.firstbankonline.com/onlinebanking>**

**We sincerely regret any inconvenience.**

**Christopher Johnson  
Head of Online Banking**