

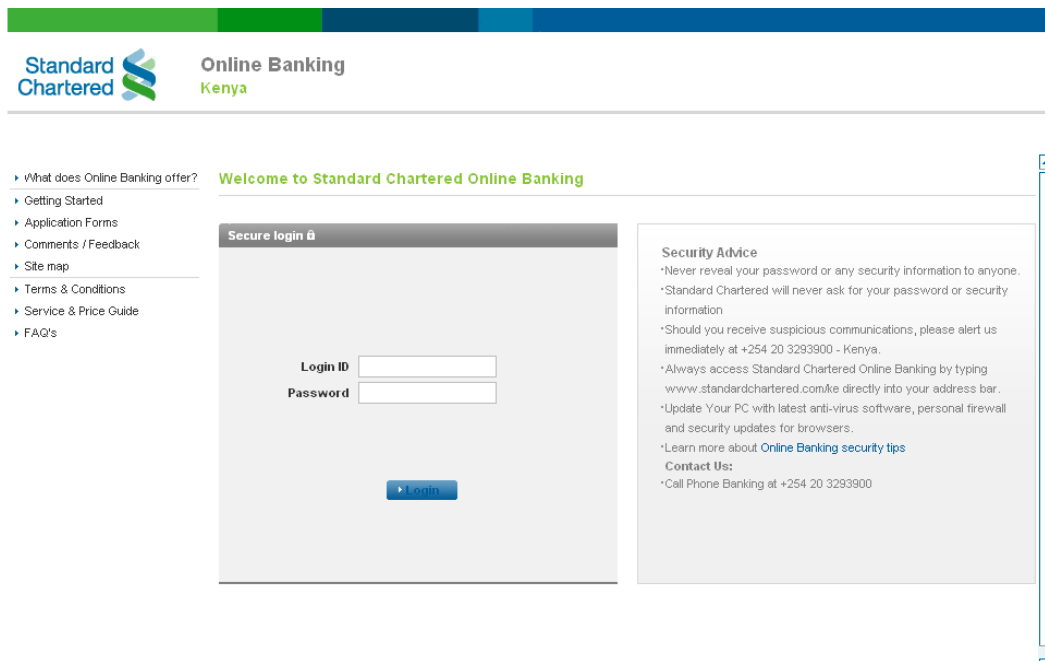
| Malware Alert |

Standard Chartered is committed to protecting you, your money, and your important personal information.

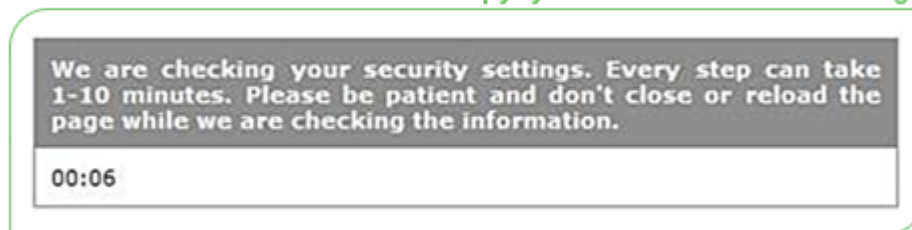
Malware is designed to steal user information by altering the look and feel of the Bank's website. Recently, we have discovered a new malware program called "SpyEye" which targets Online Banking users' transactions, specifically with regard to beneficiary addition.

Q1. How do I know if my computer is infected with malware?

If your computer has been infected with the "SpyEye" malware, you will be redirected to a page stating **"We are checking your security settings. Every step can take 1-10 minutes. Please be patient and don't close or reload the page while we are checking the information"** (sample screenshot below).



SpyEye Malware-Infected message



Q2. What should I do if my screen shows the above?

If you encounter a message similar to the above, your computer is likely to be infected with the "SpyEye" malware. You are advised to close your browser immediately and inform the Bank through our 24-hour Phone Banking Service Line on **+254 20 3293900**. You are also advised to refrain from using this computer for Online Banking until it has been checked and cleared of the malware.

Q3. What should I do to keep my information safe online?

- Check that your antivirus software is up to date.
- For your security, do not click on links from emails, install any programs from doubtful origins or perform online transactions on computers that you suspect are compromised.
- Always access our Online Banking service by typing in the correct URL (<http://www.standardchartered.co.ke>)
- Other [security tips](#).