CIMB Clicks – Public FAQ

Monday, 17 December 2018

---

1. **We heard this news online with regards to security of CIMB Clicks. Is this true?**
   We would like to confirm that the news related to the online security of CIMB Clicks is untrue. Our platform remains safe and all customer transactions continue to be protected.

reCAPTCHA Related:

2. **Why am I now required to complete a reCAPTCHA before being able to log-in to my CIMB Clicks?**
   reCAPTCHA is a service from Google that helps protect websites from spam and abuse. As part of our ongoing efforts to strengthen our online security, we have included a reCAPTCHA validation. Once customer has validated it successfully, they can proceed to log-in to CIMB Clicks.

3. **How does a reCAPTCHA work?**
   A "CAPTCHA" helps to tell a human and a bot apart. It is easy for human to solve, but hard for "Bots" and other malicious software to figure out.

4. **Have there been any recent security attacks on CIMB Clicks?**
   This is just a **preventive measure** to strengthen our online security. The introduction of a reCAPTCHA is part of the bank's ongoing efforts to increase the security of CIMB Clicks and safeguard our customers from any potential security threats. There is nothing to be worried about. We can assure you that CIMB Clicks and your banking transactions remain safe.

5. **Will I need to go through reCAPTCHA each time I login?**
   CIMB has deployed an invisible reCAPTCHA which will be prompted in the event the system suspects that the login is being performed by a Bot. This is just an additional measure- please do not be worried. We can assure you that CIMB Clicks and your banking transactions remain safe.

6. **Is CIMB the only bank using reCAPTCHA?**
   We are unable to comment on the practice of other banks. To us your security is of utmost importance, which is why we have ongoing efforts to strengthen our online security.

Password Related:

7. **I noticed that I am still able to log-in to my CIMB Clicks despite adding a few invalid characters (more than 8 characters) after my password. May I know why?**
   You are experiencing this due the way the Clicks Password Rule is designed. We can assure you that CIMB Clicks and your banking transactions remain safe.

Clicks Password Rule	Scenario : Customer keys in additional characters	Example
For passwords set **before** 18th November 2018 • The password length must be 8 characters • No requirement on special character	The system only looks at the exact number of characters of your password to validate login and ignores the rest.	Password is "abcd1234" – i.e. length is 8 characters but the customer keys in "abcd1234@#" • the system will only read "abcd1234" and ignore the " @#" • The customer is still able to log in.
For passwords set **on/after** 18th November 2018 • Password length must be between 8 -20 characters. • Must use a combination of letters, numbers, and special characters (refer to Q10 for guidance)	The system does not allow the customer to login when they key in any additional characters.	Password is "abcd1234" – i.e. length is 8 characters but the customer keys in 10 characters i.e. "abcd1234@#" • The system **does not allow** the customer to login • An error message of "**invalid userID or password [CLK00619]**" appears.

To avoid any concerns regarding the login, we encourage you to change your password, if you have not already done so.

Clicks Security:

8. **How do I know that my Clicks account is not compromised?**
   Ensuring your online security is a **joint effort** by both the bank and customer.
   On our part the Bank has taken the following proactive steps:
   - Our system will only allow you to perform financial transactions with a valid TAC.
   - We have 24 hour ongoing fraud monitoring and control systems in place to safeguard our customers.
   - Introduced the use of reCAPTCHA as an additional authentication to enhance customer's security.
   - Enhanced our password security to accept passwords longer than eight (8) characters.

   As a customer, we would like to encourage you to safeguard your CIMB Clicks security by taking the following steps:
   - **Do** change your password regularly
   - **Do** have a password of 8 characters or more using a combination of letters, numbers, and special characters
   - **Do not** disclose your password and TAC to anyone.
   - **Do not** use your Clicks user ID as your password**.**

9. **How is CIMB ensuring that my Clicks account is not being compromised?**
   We have an IT security team that monitors any suspicious activities on CIMB Clicks. They will take the necessary appropriate action should they detect any suspicious activities on CIMB Clicks.

10. **Do I need to take any action to protect myself?**
    As a customer, we would like to encourage you to safeguard your CIMB Clicks security by taking the following steps:
    - **Do** change your password regularly
    - **Do** have a password of 8 characters or more using a combination of letters, numbers, and special characters
    - **Do not** disclose your password and TAC to anyone.
    - **Do not** use your Clicks user ID as your password**.**

11. **If I suspect my account has been compromised, what should I do?**
    Please call our contact centre at 03- 62047788 or write to us at cru@cimb.com. We will look into the issue and handle it accordingly.