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 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.

Debit Card/ PayPal related queries

12. **Are the unauthorized transactions on PayPal/ Debit Cards posted by some of your customers related to Clicks?**
    We can confirm that these are matters separate from CIMB Clicks.

13. **Why do some websites such as PayPal not require an OTP?**
    The use of OTP is a policy adopted by e-commerce site owners. Whilst online transactions on Malaysian websites require an OTP (called 3D authentication), many international websites such as Facebook or PayPal do not require an OTP (called Non-3D transactions). Allowing both 3D and non-3D transactions are a common industry practice for all banks and not unique to CIMB. Customers can also use their Debit Cards to perform international online transactions via the internet by opting in for this service.

14. **Is there an increase in unauthorized transactions on Debit Cards?**
    Our continuous monitoring suggests that everything is as per normal levels. Customers who notice any irregularity in their statement should raise the matter through any of our official channels. If there is any irregularity for non-3D transactions, subject to a verification process the transaction amount will be credited back into the customer's account within 14 days.

CIMB Clicks – Soalan Lazim

Isnin, 17 Disember 2018

---

1. **Kami terdengar berita mengenai isu keselamatan CIMB Clicks. Adakah ini benar?**
   CIMB ingin mengesahkan bahawa berita yang berkaitan dengan keselamatan dalam talian CIMB Clicks adalah tidak benar. Platform kami selamat dan semua transaksi pelanggan terus dilindungi.

Berkaitan reCaptcha:

2. **Mengapakah saya kini perlu melengkapkan reCaptcha sebelum dapat log masuk ke CIMB Clicks?**
   reCapthcha merupakan perkhidmatan Google yang membantu melindungi laman web dari ancaman spam dan penyalahgunaan. Tambahan reCaptcha ke dalam sistem adalah sebahagian daripada usaha berterusan kami untuk mengukuhkan keselamatan dalam talian. Setelah pelanggan berjaya melalui pengesahan **reCaptcha**, maka pelanggan boleh meneruskan log masuk ke CIMB Clicks.

3. **Bagaimanakah reCaptcha berfungsi?**
   "Captcha" membantu membezakan pengguna manusia dari bot. Ianya mudah untuk diselesaikan oleh manusia tetapi sukar bagi bot dan perisian jahat untuk melepasinya.

4. **Pernahkah terdapat sebarang serangan keselamatan ke atas CIMB Clicks?**
   Ini adalah sebagai **langkah pencegahan** bagi memperkukuhkan keselamatan sistem dalam talian kami. Pengenalan reCaptcha merupakan sebahagian daripada usaha berterusan bank untuk meningkatkan keselamatan CIMB Clicks dan bagi melindungi para pelanggan kami dari ancaman keselamatan siber. Tiada apa yang perlu dibimbangkan. Kami memberi jaminan bahawa CIMB Clicks dan urus niaga perbankan anda kekal selamat.

5. **Adakah saya perlu melalui reCaptcha setiap kali log masuk?**
   reCaptcha yang diaftifkan tidak kelihatan kecuali apabila sistem mengesyaki bahawa log masuk sedang dilakukan oleh bot. Pelanggan tidak perlu risau, kerana ini hanyalah langkah tambahan. Kami memberi jaminan bahawa CIMB Clicks dan urus niaga perbankan anda kekal selamat.

6. **Adakan CIMB satu-satunya bank yang menggunakan fungsi reCaptcha?**
   Kami tidak dapat mengulas mengenai amalan bank lain. Bagi kami, keselamatan transaksi anda amat penting maka inilah sebabnya kami terus berusaha untuk memperkukuhkan keselamatan dalam talian kami.

Berkaitan kata laluan:

7. **Saya perasan yang saya masih boleh log masuk ke CIMB Clicks walaupun dengan tambahan beberapa aksara tidak sah (lebih daripada 8 aksara) selepas kata laluan saya. Bolehkah saya tahu mengapa?**
   Anda melalui pengalaman ini disebabkan oleh Peraturan Kata Laluan Clicks. Kami memberi jaminan bahawa CIMB Clicks dan urus niaga perbankan anda kekal selamat

Peraturan Kata Laluan Clicks	Senario: Pelanggan memasukkan aksara tambahan	Contoh
Bagi kata laluan yang ditetapkan **sebelum** 18 November 2018 • Kata laluan mestilah sepanjang 8 aksara • Tidak perlu menggunakan aksara khas	Sistem hanya mengenali jumlah aksara yang tepat untuk kata laluan anda bagi mengesahkan login dan mengabaikan selebihnya.	Kata laluan "abcd1234" – sepanjang 8 aksara tetapi pelanggan menaip "abcd1234@#" • Sistem akan hanya mengenali "abcd1234" dan mengabaikan "@#" • Pelanggan masih boleh log masuk.
Bagi kata laluan yang ditetapkan **pada**/**selepas** 18 November 2018 • Kata laluan mestilah sepanjang 8 -20 aksara. • Perlu menggunakan kombinasi abjad, nombor dan aksara khas (rujuk Soalan 10 untuk panduan)	Sistem tidak membenarkan pengguna untuk log masuk jika terdapat aksara berlebihan.	Kata laluan "abcd1234" – sepanjang 8 aksara tetapi pelanggan menaip "abcd1234@#" • Sistem **tidak membenarkan** pelanggan untuk log masuk • Sebuah mesej ralat "**invalid userID or password [CLK00619]**" akan muncul.

Untuk mengelakkan kebimbangan mengenai log masuk, kami menggalakkan anda menukar kata laluan, jika anda belum melakukannya.

Keselamatan Clicks:

8. **Bagaimanakah untuk saya mengetahui jika akaun Clicks saya tidak dikompromi?**
   Keselamatan dalam talian merupakan usaha bersama oleh kedua-dua pihak bank dan pelanggan. Di pihak kami, Bank telah mengambil langkah-langkah proaktif berikut:
   - Sistem kami hanya membenarkan transaksi kewangan dengan TAC yang sah.
   - Kami mempunyai sistem pemantauan dan kawalan penipuan 24 jam untuk melindungi pelanggan.
   - Pengenalan fungsi reCaptcha sebagai langkah pengesahan tambahan untuk meningkatkan keselamatan pelanggan.
   - Meningkatkan keselamatan kata laluan untuk menerima kata laluan lebih daripada lapan (8) aksara.

   Kami menggalakkan pelanggan kami untuk melindungi keselamatan akaun CIMB Clicks masing-masing dengan mengambil langkah-langkah berikut:
   - **Sila** tukar kata laluan anda dengan kerap
   - **Sila** tetapkan kata laluan sepanjang 8 aksara atau lebih, menggunakan gabungan abjad, nombor dan aksara khas
   - **Jangan** dedahkan kata laluan dan TAC anda kepada sesiapa
   - **Jangan** gunakan ID pengguna Clicks (*User ID*) sebagai kata laluan anda**.**

9. **Bagaimanakah CIMB memastikan bahawa akaun Clicks saya tidak dikompromi?**
   Kami mempunyai pasukan keselamatan IT yang memantau sebarang aktiviti yang mencurigakan pada CIMB Clicks. Mereka akan mengambil tindakan yang sewajarnya jika terdapat sebarang aktiviti yang mencurigakan dikesan pada CIMB Clicks.

10. **Adakah saya perlu mengambil sebarang langkah untuk melindungi diri saya?**
    Kami menggalakkan pelanggan untuk melindungi keselamatan CIMB Clicks masing-masing dengan mengambil langkah-langkah berikut:
    - **Sila** tukar kata laluan anda dengan kerap
    - **Sila** tetapkan kata laluan sepanjang 8 aksara atau lebih, menggunakan gabungan abjad, nombor dan aksara khas
    - **Jangan** dedahkan kata laluan dan TAC anda kepada sesiapa
    - **Jangan** gunakan ID pengguna Clicks (*User ID*) sebagai kata laluan anda**.**

11. **Jika saya mengesyaki akaun saya telah dikompromi, apakah yang perlu saya lakukan?**
    Sila hubungi pusat pelanggan kami di 03- 62047788 atau menulis kepada kami di cru@cimb.com. Kami akan menangani isu ini dengan sewajarnya.

Berkenaan Persoalan Kad Debit/PayPal

12. **Adakah urus niaga tanpa kebenaran dari PayPal/Kad Debit seperti yang diutarakan beberapa pelanggan berkaitan dengan Clicks?**
    Kami mengesahkan yang perkara ini tiada kaitan dengan isu CIMB Clicks.

13. **Mengapakah beberapa lawan web seperti PayPal tidak memerlukan OTP?**
    Penggunaan OTP adalah dasar yang digunapakai oleh pemilik tapak e-dagang. Walaupun urus niaga dalam talian di laman web di Malaysia memerlukan OTP (dipanggil pengesahan 3D), banyak laman web antarabangsa seperti Facebook atau PayPal tidak memerlukan OTP (atau transaksi bukan 3D). Dengan membenarkan kedua-dua transaksi 3D dan bukan 3D adalah amalan industri biasa untuk semua bank dan tidak hanya unik kepada CIMB. Pelanggan juga boleh menggunakan Kad Debit mereka untuk melakukan transaksi dalam talian antarabangsa melalui internet dengan memilih (*opt in*) untuk menggunakan perkhidmatan ini.

14. **Adakah terdapat sebarang peningkatan urus niaga tanpa kebenaran pada Kad Debit?**
    Pemantauan berterusan kami menunjukkan bahawa keadaan adalah pada tahap biasa. Pelanggan yang menyedari sebarang masalah pada penyata mereka perlulah melaporkannya melalui saluran rasmi kami. Jika terdapat sebarang masalah pada urus niaga bukan 3D, dan ianya telah melalui proses pengesahan, amaun transaksi akan dikreditkan semula ke dalam akaun pelanggan dalam masa 14 hari.

CIMB Clicks 公众常见问题

2018 年 12 月 17 日

---

1. **我们在网络新闻听到关于 CIMB Clicks 的安全问题？这是真的吗？**
   我们确认 CIMB Clicks 网络安全问题的新闻是不确实的。我们的平台仍然安全及所有客户的交易持续获得保护。

<u>关于验证码：</u>

2. **为何在未登入自身的 CIMB Clicks 之前，我必须完成验证码核实？**
   验证码是源自谷歌的一项服务，可协助保护网站被入侵及滥用。在强化我们网络安全方面，我们加入了验证码核实。一旦客户成功核实身份，他们可以继续登入 CIMB Clicks。

3. **验证码如何操作？**
   “验证码”协助区分人类及机器人。人类可以轻易辨识及解答它，不过“机器人”及其他恶意软件却无法辨识。

4. **CIMB Clicks 日前是否曾经受到入侵？**
   这仅是强化我们网络安全的**防御性**措施。推介验证码是银行持续强化 CIMB Clicks 网络安全的部分努力，保护客户免受任何网络安全的威胁。请勿过于担忧。我们可以保证 CIMB Clicks 及您的银行交易仍然安全。

5. **每次登入时，我是否需要通过验证码核实？**
   联昌银行采用隐形式的验证码核实，当系统对登入者产生怀疑时验证码将会起动。这是项附加措施，请勿担忧。我们保证 CIMB Clicks 及您的银行交易仍然安全。

6. **CIMB 是唯一使用验证码核实的银行？**
   我们不能对其他银行的做法作出回应。对我们而言安全为首要考量，这是为何我们持续对强化网络安全付出努力。

关于密码：

7. **虽然在输入密码之后加入一些多余字母（超过 8 个代号），我发现我仍然可以登入 CIMB Clicks。我可以知道是什么原因吗？**
   这是因为 Clicks 所设定的密码条例方式。我们保证您的 CIMB Clicks 及银行交易仍然安全。

Clicks 密码条例	案例：客户输入多余代号	例子
密码设定于 2018 年 11 月 18 日之前 • 密码的长度一定是8个代号 • 无需特别符号	核实登入时，系统将只专注于您密码的代号并忽略其余代号。	密码为“abcd1234” – 长度为 8 个代号，不过客户输入“abcd1234@#” • 系统只解读“abcd1234”并忽略“ @#” • 客户仍然可以登入。
密码设定于 2018 年 11 月 18 日或之后 • 密码长度定为8至20个代号。 • 一定需要使用字母、数字及特别符号。 (可参阅第 10 道题)	当客户输入多余代号，系统将不允许他们登入。	密码为“abcd1234” – 长度为 8 个代号不过客户输入 10 个代号，例如“abcd1234@#” • 系统**不允许**客户登入 • 将出现“用户身份或密码无效**[CLK00619]**”的错误输入讯息。

为了避免对登入存有任何疑惑，我们鼓励您更新密码。

关于 Clicks 的安全：

8. **我如何知道我的 Clicks 户口没有受到连累？**
   银行与客户之间必须**相互**努力保证网络安全。
   银行已经采取以下的积极步骤：
   - 我们的系统将只允许您使用有效的 TAC 进行金融交易。
   - 我们具备持续性的欺诈监管及控制系统来保护我们的客户。
   - 使用验证码作为附加核实措施来强化客户的安全。
   - 强化密码安全性，包括接受超过 8 个代号的密码。

   作为客户我们鼓励您采取以下步骤保护 CIMB Clicks 的安全:

- **经常性更新密码**
- **使用 8 个或更多的代号，包括结合字母、数字及特别代号。**
- **勿向任何人透露您的密码及 TAC。**
- **勿使用 Clicks 用户代号作为密码。**

9. 联唱银行如何确保我的 Clicks 户口没有受到连累？

我们拥有资讯科技安全队伍监督于 CIMB Clicks 出现的任何可疑活动。若发现任何可疑活动，他们将会采取必要的应对行动。

10. 我需要采取什么行动来保护自己？

作为客户我们鼓励您采取以下步骤保护 CIMB Clicks 的安全:

- **经常性更新密码**
- **使用 8 个或更多的代号，包括结合字母、数字及特别代号。**
- **勿向任何人透露您的密码及 TAC。**
- **勿使用 Clicks 用户代号作为密码。**

11. 要是怀疑自身户口受到连累，我该怎么做？

请拨打 03- 62047788 予客服中心或电邮 cru@cimb.com。我们将会处理相关问题并妥善解决。

关于扣账卡/PayPal 相关问题:

12. 部分客户所发布的 PayPal/ 扣账卡未经授权交易是否与 Clicks 有关？

我们可以确认这些事项与 CIMB Clicks 是不相关的。

13. 为何一些网站例如 PayPal 不需要一次性密码（OTP）？

使用 OTP 是电子商务业者所采用的模式。虽然马来西亚网站的网络交易需要 OTP (称之为三维验证)，但很多国际网站例如脸书或 PayPal 并不需要 OTP (称之为非三维验证)。联昌银行乃至所有银行都会允准三维及非三维验证交易的普遍业界常规。客户可以在互联网选择纳入此项服务，使用扣账卡进行国际网络交易。

14. 扣账卡的未经授权交易是否有所增加?

根据我们的观察，一切运作处于正常状态。若发现任何不寻常的账目，可以通过任何正式管道寻求解决。若非三维交易出现不寻常，只要通过验证程序，交易数额将会在 14 天内汇入客户账户。