CẨM NANG HƯỚNG DẪN GIAO DỊCH AN TOÀN KHI GIAO DỊCH THẺ

STT	Câu hỏi	Trả lời
1	**Vietcombank có những loại thẻ nào?**	Thẻ ngân hàng là một phương tiện thanh toán giúp cho Khách hàng có thể thực hiện được các giao dịch như rút tiền tại ATM, thanh toán tại các cửa hàng, siêu thị, nhà hàng, khách sạn, thanh toán tại các website/ứng dụng bán hàng trực tuyến … Vietcombank là ngân hàng đầu tiên cung cấp dịch vụ thẻ tại Việt Nam, và hiện tại, là ngân hàng có danh mục các sản phẩm thẻ đa dạng đứng đầu thị trường với 02 nhóm sản phẩm chủ yếu như sau: • **Thẻ tín dụng**: Là thẻ được sử dụng để chi tiêu trước, trả tiền sau trong một hạn mức nhất định do ngân hàng cấp, với thời gian miễn lãi có thể lên đến 55 ngày. Vietcombank là ngân hàng duy nhất phát hành 5 thương hiệu thẻ tín dụng: American Express, Visa, MasterCard, JCB và UnionPay. • **Thẻ ghi nợ**: Là thẻ cho phép Khách hàng thực hiện giao dịch thẻ trong phạm vi số tiền và hạn mức thấu chi (nếu có) trên tài khoản thanh toán của Khách hàng mở tại ngân hàng. Xét về phạm vi, thẻ ghi nợ được chia thành: – ***Thẻ ghi nợ nội địa***: được sử dụng để thực hiện giao dịch trong nước. – ***Thẻ ghi nợ quốc tế***: được sử dụng để thực hiện giao dịch trong nước và trên thế giới.
2	**Khách hàng có thể làm gì với một chiếc thẻ ngân hàng của Vietcombank?**	Với một chiếc thẻ của Vietcombank, Khách hàng có thể thực hiện được các giao dịch thanh toán tiện ích, đa dạng, linh hoạt, mọi lúc, mọi nơi ở phạm vi trong nước và trên toàn thế giới, bao gồm: – **Giao dịch tại ATM**: Rút tiền mặt, vấn tin tài khoản, in sao kê tài khoản, chuyển tiền, thanh toán hóa đơn cho các dịch vụ điện, học phí, viễn thông, bảo hiểm, vé máy bay… – **Giao dịch tại các điểm chấp nhận thẻ (POS):** Thanh toán linh hoạt tại mạng lưới hàng trăm ngàn POS trong nước và hàng triệu POS trên toàn thế giới.

		– **Giao dịch trên internet và các ứng dụng di động:** Mua hàng trực tuyến tiện lợi tại nhiều website, thanh toán qua các ứng dụng di động như Samsung Pay, MOCA, liên kết thẻ với các Ví điện tử như Moca.
3	**Các rủi ro có thể xảy ra khi giao dịch bằng thẻ?**	Vì thẻ là một thiết bị vật lý do Khách hàng tự bảo quản và các giao dịch thẻ là giao dịch do Khách hàng tự thực hiện**,** nên có thể xảy ra rủi ro khi Khách hàng mất/thất lạc thẻ hoặc bị đánh cắp thông tin thẻ. Ngoài ra, với sự gia tăng mạnh mẽ của các giao dịch thanh toán thẻ trực tuyến, các rủi ro liên quan đến lừa đảo/đánh cắp thông tin trực tuyến cũng có thể xảy đến với Khách hàng, cụ thể như sau: **1. Khách hàng bị mất hoặc thất lạc thẻ** Khi đó, ngươi nhặt được thẻ/kẻ gian ăn cắp thẻ có thể sử dụng thẻ tại POS hoặc chi tiêu trên internet tại một số website không yêu cầu xác thực bằng 3D-SECURE. **2. Khách hàng bị lừa đảo đánh cắp thông tin** *a. Thủ đoạn lấy cắp thông tin trực tiếp* – Kẻ gian cài đặt thiết bị skimming (công cụ quét dữ liệu) hoặc đặt camera bí mật tại các ATM để đánh cắp thông tin thẻ của Khách hàng. Ngoài ra, kẻ gian còn có thể sử dụng máy ảnh nhiệt. Chúng sẽ chụp lại màn hình để tìm ra dấu hiệu nhiệt từ tay của Khách hàng để để tìm ra mã PIN. Ngoài ra, kẻ gian cũng có thể đánh cắp thông tin dữ liệu thẻ qua việc cài đặt phần mềm độc hại vào máy ATM. – Kẻ gian là nhân viên của những đơn vị chấp nhận thẻ. Khi Khách hàng đưa thẻ để thanh toán, kẻ gian bí mật đánh cắp thông tin thẻ của Khách hàng. – Khách hàng giao dịch trực tuyến tại các ĐVCNT thẻ trực tuyến và bị tội phạm lấy cắp thông tin số thẻ, ngày hiệu lực và/hoặc CVV/CVC của chủ thẻ thật để thực hiện giao dịch giả mạo trên tại các ĐVCNT trực tuyến. *b. Thủ đoạn lấy cắp thông tin gián tiếp* *(b.1). Các thủ đoạn lừa đảo lấy cắp thông tin dịch vụ ngân hàng*

		Đối tượng lừa đảo tìm cách lấy cắp các thông tin dịch vụ ngân hàng của Khách hàng, từ đó truy cập và chiếm đoạt tiền từ tài khoản. Một số hình thức lấy cắp thông tin phổ biến bao gồm: • **<u>Nhóm thủ đoạn giả mạo website/fanpage</u>** – Đối tượng lừa đảo mạo danh là người thân/người quen và thông báo sẽ chuyển tiền cho Khách hàng. Đối tượng gửi cho Khách hàng đường link giả mạo (thường giả mạo website ngân hàng, website công ty chuyển tiền quốc tế …) và yêu cầu xác nhận thông tin. Khách hàng truy cập vào link giả mạo và cung cấp cho đối tượng các thông tin về dịch vụ ngân hàng điện tử (tên truy cập, mật khẩu, mã OTP) hoặc dịch vụ thẻ (số thẻ, ngày hiệu lực, CVV/CVC-mã số bảo mật của thẻ, mã OTP). – Đối tượng lừa đảo lập fanpage trên mạng xã hội để mạo danh ngân hàng/tổ chức cung cấp dịch vụ Ví điện tử. Các fanpage này thường sử dụng logo, hình ảnh và các bài viết được sao chép từ fanpage chính thức. Đối tượng lừa đảo tiếp cận Khách hàng để tư vấn sản phẩm dịch vụ và yêu cầu Khách hàng cung cấp thông tin cá nhân, công việc, thu nhập… để phục vụ mục đích gian lận hoặc hướng Khách hàng sang các dịch vụ tín dung đen. – Đối tượng lừa đảo mua các tên miền website có địa chỉ gây nhầm lẫn với địa chỉ mà Khách hàng muốn truy cập (có thể chỉ cần khác nhau một ký tự trên domain) và thiết kế giao diện trong trang giống hệt với website thật khiến Khách hàng nhầm tưởng đó là website chính thức. Từ đó, đánh cắp được các dữ liệu khi Khách hàng nhập vào đó. – Đối tượng lừa đảo giả mạo tin nhắn trúng thưởng, tin nhắn cảnh báo, yêu cầu Khách hàng gửi thông tin thẻ hoặc bấm vào các đường link đi kèm và nhập thông tin dịch vụ cho kẻ gian. – Đối tượng lừa đảo mạo danh ngân hàng/đơn vị khác gửi tin nhắn thông báo trúng thưởng và yêu cầu Khách hàng click vào đường link giả mạo. – Một số ví dụ về đường link giả mạo: http://www.www-vietcombank.com.vn/ http://www.homebank247.com/

http://mail.www-vietcombank.com.vn/
http://western-union-quocte.wixsite.com/ibanking
….

- **Nhóm thủ đoạn lừa cài đặt phần mềm gián điệp**

– Đối tượng lừa Khách hàng cài đặt phần mềm, ứng dụng gián điệp để đánh cắp thông tin của Khách hàng, trong đó có cả các thông tin về dịch vụ, thông tin về mật khẩu OTP được gửi đến điện thoại của Khách hàng.

- **Nhóm thủ đoạn giả danh**

– Đối tượng lừa đảo mạo danh nhân viên ngân hàng/nhân viên của tổ chức cung ứng dịch vụ ví điện tử yêu cầu Khách hàng xác thực thông tin để nâng cấp dịch vụ.

– Đối tượng lừa đảo mạo danh là cơ quan công an, tòa án, viện kiểm sát thông báo Khách hàng có liên quan đến vụ án buôn lậu/rửa tiền/mua bán ma túy và yêu cầu Khách hàng cung cấp thông tin về dịch vụ để phục vụ công tác điều tra.

Đối với các thủ đoạn này, Quý Khách hàng hãy lưu ý một số nguyên tắc sau đây để đảm bảo an toàn:

- Một là: VCB chỉ có một website chính thức với địa chỉ là https://portal.vietcombank.com.vn/. Trang fanpage chính thức của VCB có địa chỉ https://www.facebook.com/ilovevcb/ (có dấu tích xanh của Facebook).
- Hai là: Kiểm tra kỹ các phần mềm/ứng dụng trước khi cài đặt. Luôn sử dụng phần mềm bảo mật từ các hãng cung cấp uy tín.
- Ba là: Vietcombank không bao giờ gửi đường link hoặc liên hệ Khách hàng để yêu cầu Khách hàng cung cấp thông tin bảo mật dưới mọi hình thức. Vì vậy, các yêu cầu cung cấp thông tin (nếu có) đều là giả mạo, Khách hàng tuyệt đối không cung cấp thông tin khi nhận được các yêu cầu này.

		(b2). Các thủ đoạn lừa đảo Khách hàng tự chuyển tiền – Đối tượng giả mạo người thân, bạn bè nhờ Khách hàng chuyển tiền. – Đối tượng lừa đảo mạo danh là nhân viên bưu điện thông báo Khách hàng bị nợ cước viễn thông, hoặc Khách hàng có bưu kiện, yêu cầu Khách hàng phải chuyển tiền để thanh toán cước viễn thông hoặc chuyển tiền cước phí vận chuyển bưu kiện hoặc cước lưu kho. – Đối tượng lừa đảo mạo danh là cơ quan công an, tòa án, viện kiểm sát thông báo Khách hàng có liên quan đến vụ án buôn lậu/rửa tiền/mua bán ma túy và yêu cầu Khách hàng chuyển tiền tới tài khoản của cơ quan công an (giả mạo) để tạm giữ, phục vụ công tác điều tra. – Đối tượng lừa đảo mạo danh nhân viên ngân hàng/ nhân viên các công ty lớn (như công ty viễn thông)/ nhân viên tổ chức cung ứng dịch vụ ví điện tử thông báo Khách hàng trúng thưởng, và yêu cầu Khách hàng chuyển tiền phí để nhận thưởng. **Đối với các thủ đoạn này, Quý Khách hàng hãy nâng cao cảnh giác, xác định chính xác thông tin của người liên hệ. Không thực hiện chuyển tiền, cung cấp thông tin cá nhân cho người lạ qua điện thoại. Đồng thời, báo cho cơ quan Công an/cơ quan chức năng nơi gần nhất nếu thấy dấu hiệu nghi ngờ.**
4	**Ngân hàng bảo vệ tôi như thế nào?**	Với hàng triệu giao dịch mỗi ngày, sự an toàn trong mỗi giao dịch của Khách hàng là mối quan tâm lớn nhất của Vietcombank. Chúng tôi đang áp dụng rất nhiều các giải pháp vượt trội để bảo vệ cho các giao dịch của Khách hàng như: **1) Áp dụng tiêu chuẩn bảo mật dữ liệu PCI DSS** – Vietcombank đã được cấp Chứng nhận Bảo mật quốc tế PCI DSS *(Payment Card Industry Data Security Standard)*. PCI DSS là tiêu chuẩn bắt buộc đối với bất kỳ tổ chức, doanh nghiệp có liên quan đến nghiệp vụ xử lý, truyền tải và lưu trữ dữ liệu thẻ thanh

toán. PCI DSS là chứng nhận bảo mật có yêu cầu khắt khe nhất trong ngành thanh toán, có giá trị trên toàn cầu.

- Để đạt tiêu chuẩn Bảo mật quốc tế PCI DSS, doanh nghiệp phải đáp ứng 12 nhóm yêu cầu chính với hơn 100 yêu cầu chi tiết, bao gồm 6 nhóm mục tiêu: Xây dựng và duy trì hệ thống mạng bảo mật; Bảo vệ dữ liệu thẻ thanh toán; Xây dựng và duy trì an ninh mạng; Xây dựng hệ thống kiểm soát xâm nhập; Theo dõi và đánh giá hệ thống thường xuyên; Chính sách bảo vệ thông tin.

2) Áp dụng tiêu chuẩn thẻ chip EMV

- EMV là tiêu chuẩn thẻ thanh toán thông minh do 3 liên minh thẻ lớn nhất thế giới là Europay, MasterCard và Visa cùng phát triển. Thẻ chip EMV giúp tăng cường sự an toàn và yên tâm trong giao dịch, không lo sợ bị sao chép, mất dữ liệu vì thẻ được gắn chip điện tử với bộ vi xử lý như một máy tính thu nhỏ đa chức năng và ứng dụng, có khả năng lưu trữ các thông tin quan trọng được mã hóa với độ bảo mật cao.

- Hiện nay, tất cả các thẻ quốc tế của Vietcombank đã được phát hành với chuẩn EMV. Vietcombank cũng đang trong quá trình chuyển đổi các thẻ nội địa theo tiêu chuẩn khắt khe này.

3) Công nghệ Tokenization cho các giao dịch trực tuyến

- Công nghệ Tokenization mã hóa số thẻ thành Token (những dãy ký tự đặc biệt) nhằm chống sao chép thẻ vì kẻ gian không thể truy cập được vào dữ liệu thẻ thực sự, đồng thời tự động lưu số thẻ đã mã hóa để giúp Khách hàng không phải nhập lại thông tin thẻ cho lần mua hàng tiếp theo mà chỉ cần xác thực để hoàn tất giao dịch.

- Mã Token này được sử dụng thay cho thông tin thẻ trong các giao dịch sau này, đảm bảo an toàn tuyệt đối. Nếu xảy ra lỗ hổng dữ liệu, kẻ gian sẽ không thể truy cập được vào dữ liệu thẻ thật sự, bởi những mã Token được lưu trong hệ thống sẽ chỉ có giá trị duy nhất với đơn vị thanh toán hợp pháp.

4) Bảo mật bằng 3D-SECURE cho các giao dịch trực tuyến

		– 3D-Secure là một lớp bảo vệ tăng cường cho các chủ thẻ của Vietcombank khi giao dịch trực tuyến. Với phương thức này, khi thực hiện các giao dịch trên các website thương mại điện tử có biểu tượng 3D-SECURE, bên cạnh các bước xác thực thông thường, Vietcombank sẽ gửi thêm mật khẩu giao dịch một lần (OTP) qua tin nhắn hoặc email để Khách hàng nhập và hoàn tất giao dịch. 3D-SECURE đảm bảo rằng chỉ có Khách hàng, với tư cách là chủ thẻ, sẽ có mật khẩu để hoàn tất giao dịch đó. – Là một giải pháp ưu việt, 3D-SECURE được các Tổ chức thẻ quốc tế (TCTQT) áp dụng và có tên gọi khác nhau đối với mỗi TCTQT như Safe Key (Amex), Verified by Visa (Visa), Mastercard SecureCode hoặc Master ID check (Mastercard), J-Secure (JCB). *Hiện tại, Vietcombank áp dụng 3D-SECURE cho tất cả các chủ thẻ quốc tế có đăng ký dịch vụ này.* **5) Hệ thống camera giám sát 24/7 tại các ATM** Vietcombank đã đầu tư lắp đặt hệ thống camera giám sát 24/7 hiện đại tại các phòng máy ATM trải dài trên toàn quốc để quan sát khu vực Khách hàng giao dịch, giúp phát hiện và xử lý các sự cố và xác định giao dịch gian lận … Đặc biệt, hệ thống giám sát này còn giúp phát hiện các trường hợp tội phạm sử dụng công nghệ cao để gắn thiết bị đánh cắp thông tin thẻ tại ATM. **6) Lắp đặt các thiết bị phòng chống lấy cắp dữ liệu thẻ (anti-skimming) tại ATM.**
5	**Khi có dấu hiệu nghi ngờ bị tấn công hoặc lừa đảo, tôi phải làm gì?**	**Trường hợp phát hiện ra có dấu hiệu bị lừa đảo hoặc nghi ngờ bị lừa đảo, bị tin tặc hoặc nghi ngờ bị tin tặc tấn công, để đảm bảo an toàn, Quý khách nên thực hiện theo thứ tự ưu tiên như sau:** – Khóa dịch vụ trên các kênh trực tuyến (tham khảo các cách khóa thẻ khẩn cấp tại mục 7 dưới đây). – Đổi mật khẩu của dịch vụ đang bị kẻ gian tìm cách lấy cắp thông tin. – Gọi điện ngay cho ngân hàng theo số hotline 24/7: 1900545413

<table>
<tr>
<td></td>
<td></td>
<td>
– Nếu trong giờ hành chính, Quý khách có thể đến ngay các điểm giao dịch ngân hàng để được trợ giúp.

(Tóm tắt các kênh khóa dịch vụ tạm thời/khẩn cấp)
<table>
<tr><th rowspan="2">Loại dịch vụ</th><th colspan="5">Các kênh khóa dịch vụ</th></tr>
<tr><th>Quầy giao dịch</th><th>Gọi đến 1900545413</th><th>VCB Digibank trên trình duyệt web</th><th>VCB Digibank trên ứng dụng mobile</th><th>Gửi SMS tới 6167</th></tr>
<tr><td>VCB Digibank trên trình duyệt web</td><td>✓</td><td>✓</td><td></td><td></td><td></td></tr>
<tr><td>VCB Digibank trên ứng dụng mobile</td><td>✓</td><td>✓</td><td>✓</td><td></td><td></td></tr>
<tr><td>Thẻ</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td><td>✓</td></tr>
</table>
Ngoài ra, chúng tôi khuyến nghị Quý Khách trình báo vấn đề của mình với các cơ quan có thẩm quyền (ví dụ: Công an quận/huyện/tỉnh …)
</td>
</tr>
<tr>
<td>6</td>
<td>Để hạn chế các rủi ro như nêu trên, tôi cần phải làm gì?</td>
<td>
Để đảm bảo an toàn cho các giao dịch thẻ, Vietcombank khuyến cáo Khách hàng thực hiện một số nguyên tắc sau:

1. <u>Trước và sau khi nhận thẻ</u>

– Đọc kỹ Hợp đồng sử dụng thẻ trước khi ký vào Đơn phát hành và Hợp đồng sử dụng thẻ.

– Kiểm tra các thông tin trên thẻ để đảm bảo đúng các thông tin Khách hàng đã đăng ký khi nhận thẻ tại Chi nhánh ngân hàng.
</td>
</tr>
</table>

		– Đổi mã số cá nhân (PIN) đối với các thẻ ghi nợ mà Ngân hàng cung cấp tại máy ATM ngay sau khi nhận thẻ để kích hoạt thẻ. Chú ý, Khách hàng nên tránh các con số có liên quan đến các thông tin cá nhân như: Ngày tháng năm sinh, số điện thoại, biển số xe… để tránh việc lộ thông tin cho kẻ xấu lợi dụng. **2. <u>Bảo quản thẻ</u>** – Không đưa thẻ của mình cho bất cứ người nào khác, trừ nhân viên của ngân hàng hoặc các nhân viên thu ngân của ĐVCNT được chỉ định để làm việc với Khách hàng. Khách hàng chỉ nên đưa thẻ cho nhân viên của Ngân Hàng khi thực hiện các giao dịch/thủ tục tại các điểm giao dịch của ngân hàng, không đưa thẻ ở các địa điểm bên ngoài điểm giao dịch của ngân hàng. – Không tiết lộ số PIN, số thẻ cho bất cứ ai. Khách hàng là người duy nhất được biết các thông tin đó. – Giữ thẻ cẩn thận trong ví, ở vị trí mà Khách hàng có thể dễ nhìn thấy bất cứ lúc nào Khách hàng mở ví nhằm giúp Khách hàng phát hiện sớm việc mất thẻ. – Nên đổi mã PIN thường xuyên. – Không cất giữ mã PIN chung với thẻ. – Ghi nhớ hạn mức sử dụng ngày và hạn mức rút tiền mặt đối với mỗi giao dịch của thẻ để Khách hàng có thể dễ dàng kiểm soát được khả năng chi tiêu của mình. **3. <u>Khi giao dịch tại ATM</u>** – Luôn lấy tay che bàn phím khi nhập mã PIN. – Quan sát kỹ trước khi thực hiện giao dịch tại ATM. Không giao dịch nếu máy ATM có thiết bị lạ, bất thường. – Kiểm tra kỹ vị trí đầu đọc thẻ, bàn phím, màn hình đảm bảo không có gì bất thường như vết trầy xước hoặc máng, dây điện, dấu vết băng keo trên hoặc gần đầu đọc thẻ, hoặc thiết bị gắn vào máy ATM.

		– Luôn kiểm tra tiền và lấy lại thẻ sau khi thực hiện giao dịch. Đối chiếu giao dịch in ra từ hóa đơn hoặc thông báo tại tin nhắn SMS gửi tới Khách hàng. **4. <u>Khi giao dịch tại POS</u>** – Đảm bảo giao dịch phải được thực hiện trong tầm mắt của Khách hàng để quan sát việc cà thẻ của thu ngân, yêu cầu thu ngân không được sao chụp, ghi lại các thông tin của thẻ. – Hoàn tất giao dịch qua POS bằng cách nhập mã PIN của Khách hàng (nếu có). Luôn lấy tay che bàn phím khi nhập mã PIN. – Với thẻ Chip, luôn yêu cầu thực hiện thanh toán thẻ qua đầu đọc Chip, và chỉ đồng ý thực hiện giao dịch qua dải từ trong trường hợp máy cà thẻ không có đầu đọc Chip. – Kiểm tra kỹ nội dung và tổng số tiền cần thanh toán trước khi ký tên vào hóa đơn giao dịch. – Nhận lại thẻ ngay sau khi thực hiện xong giao dịch. – Giữ lại các hóa đơn thanh toán thẻ và các chứng từ có liên quan để đối chiếu với các giao dịch trên sao kê tài khoản thẻ. – Hủy hóa đơn (xé nhỏ) trước khi vứt bỏ. **5. <u>Khi giao dịch trực tuyến</u>** – Chỉ giao dịch tại các website/ứng dụng di động uy tín, các địa chỉ mua hàng tin cậy, bảo mật cao. Lưu ý gõ địa chỉ đường link website đầy đủ vào thanh địa chỉ trong trình duyệt internet thay vì chọn đường link có sẵn hoặc được gợi ý. – Nên sử dụng máy tính cá nhân, điện thoại của mình để giao dịch thay vì các thiết bị và wifi công cộng tại công ty, quán café, quán internet… Nếu sử dụng thiết bị kết nối công cộng lưu ý tắt chế độ tự động lưu bất kỳ thông tin cá nhân, thông tin tài khoản và thẻ trên các trình duyệt.

<table>
<tr>
<td></td>
<td></td>
<td>
– Cài đặt và cập nhật các chương trình diệt virus mới nhất cho máy tính.
– Tránh cài đặt các phần mềm từ các nguồn không đáng tin cậy.
– Thường xuyên thay đổi mật khẩu và tránh sử dụng một mật khẩu cho tất cả các tài khoản.
– Tuyệt đối không lưu lại tài khoản đăng nhập và mật khẩu có gắn với thông tin thẻ trên trình duyệt khi giao dịch. Khi thực hiện hoàn tất giao dịch phải đăng xuất thoát khỏi ứng dụng, website.
– Tham khảo kỹ các điều khoản và điều kiện của website trước khi đồng ý giao dịch/thanh toán.
– Không rời khỏi màn hình/ thiết bị trong quá trình thực hiện giao dịch trực tuyến.
– Nếu phát hiện hoặc nghi ngờ thông tin, dữ liệu thẻ của mình có thể đã bị xâm nhập, vui lòng không tiếp tục giao dịch đồng thời thực hiện các biện pháp khóa thẻ khẩn cấp và liên hệ với Vietcombank để được hỗ trợ.
6. <u>Khác</u>
– Đăng ký dịch vụ nhận thông báo biến động số dư (SMS Chủ Động) để được thông báo khi phát sinh bất kỳ các giao dịch thẻ nào.
– Đăng ký dịch vụ VCB Digibank để nắm bắt thông tin giao dịch thẻ, chủ động khóa chi tiêu trực tuyến của thẻ, khóa thẻ khi có dấu hiệu nghi ngờ rủi ro và kiểm soát chi tiêu ngay trên các kênh này.
</td>
</tr>
<tr>
<td>7</td>
<td>Nếu có dấu hiệu lừa đảo, tôi có thể khóa thẻ ngay lập tức bằng cách nào?</td>
<td>
Trong trường hợp thẻ của Khách hàng bị thất lạc, mất cắp hay phát sinh giao dịch giả mạo, Quý Khách có thể chủ động khóa thẻ tạm thời qua các hình thức sau:
<table>
<tr><th>STT</th><th>Kênh thực hiện</th><th>Mô tả</th></tr>
</table>
</td>
</tr>
</table>

<table>
<tr><td></td><td></td><td>
<table>
<tr><td>Cách 1</td><td>Khóa thẻ trên ngân hàng số VCB Digibank</td><td colspan="2">Đăng nhập vào VCB Digibank >> Quản lý dịch vụ thẻ >> Khóa thẻ.</td></tr>
<tr><td rowspan="9">Cách 2</td><td rowspan="9">Gửi tin nhắn SMS tới tổng đài 6167</td><td>Khóa toàn bộ thẻ tại VCB</td><td>VCB KT TOANBO</td></tr>
<tr><td>Khóa toàn bộ thẻ Visa</td><td>VCB KT VISA</td></tr>
<tr><td>Khóa toàn bộ thẻ Master</td><td>VCB KT MASTER</td></tr>
<tr><td>Khóa toàn bộ thẻ Amex</td><td>VCB KT AMEX</td></tr>
<tr><td>Khóa toàn bộ thẻ JCB</td><td>VCB KT JCB</td></tr>
<tr><td>Khóa toàn bộ thẻ Unionpay</td><td>VCB KT UNIONPAY</td></tr>
<tr><td>Khóa toàn bộ thẻ nội địa:</td><td>VCB KT NOIDIA</td></tr>
<tr><td colspan="2">Lưu ý:
▪ Trường hợp không nhớ cú pháp cụ thể, Quý khách soạn tin nhắn theo cú pháp VCB HELP và gửi đến tổng đài 6167 để được hướng dẫn.
▪ Thẻ của Quý khách chỉ được khóa thành công khi Quý khách nhận được tin nhắn phản hồi với nội dung “Thẻ của Quý khách đã được khóa tạm thời”.</td></tr>
<tr><td>Cách 3</td><td>Tổng đài tự động 1900545413</td><td colspan="2">Khách hàng khóa thẻ bằng cách gọi điện đến số 1900545413 >> Nhấn phím 1 >> 1 >> 1 và làm theo hướng dẫn.</td></tr>
<tr><td>Cách 4</td><td>Trung tâm hỗ trợ Khách hàng 24/7</td><td colspan="2">Khách hàng kết nối với nhân viên hỗ trợ qua tổng đài 1900545413 và yêu cầu khóa thẻ.</td></tr>
</table>
</td><td></td></tr>
</table>

<table>
<tr>
<td></td>
<td></td>
<td>
<table>
<tr><td>Cách 5</td><td>Tại điểm giao dịch của Vietcombank trên toàn quốc</td><td>Khách hàng trực tiếp ra các điểm giao dịch của Vietcombank để yêu cầu khóa thẻ.</td></tr>
</table>
Vietcombank khuyến khích khách hàng khóa thẻ qua Ngân hàng số VCB Digibank hoặc tin nhắn SMS để đảm bảo thẻ được khóa nhanh nhất.
Sau khi xác định thẻ của mình đã an toàn, Quý khách có thể mở lại thẻ để sử dụng ngay trên VCB Digibank (bằng cách: Đăng nhập vào VCB Digibank >> Quản lý dịch vụ thẻ >> Mở khóa thẻ) hoặc đến trực tiếp các điểm giao dịch của Vietcombank trên toàn quốc.
</td>
</tr>
<tr>
<td>8</td>
<td>3D-SECURE là gì và tại sao tôi nên sử dụng nó?</td>
<td>
1. <u>3D SECURE là gì?</u>

3D-SECURE là một lớp bảo vệ tăng cường cho các chủ thẻ của Vietcombank khi giao dịch trực tuyến. Với phương thức này, khi thực hiện các giao dịch trên các website thương mại điện tử có biểu tượng 3D-SECURE, bên cạnh các bước xác thực thông thường, Vietcombank sẽ gửi thêm mật khẩu giao dịch một lần (OTP) qua tin nhắn hoặc email để Khách hàng nhập và hoàn tất giao dịch. 3D-SECURE đảm bảo rằng chỉ có Khách hàng, với tư cách là chủ thẻ, sẽ có mật khẩu để hoàn tất giao dịch đó.
Là một giải pháp ưu việt, 3D-SECURE được các Tổ chức thẻ quốc tế (TCTQT) áp dụng và có tên gọi khác nhau đối với mỗi TCTQT như Safe Key (Amex), Verified by Visa (Visa), Mastercard SecureCode hoặc Master ID check (Mastercard), J-Secure (JCB).

2. <u>Ai có thể được sử dụng 3D-SECURE</u>

Khách hàng cá nhân là chủ thẻ tín dụng và ghi nợ quốc tế do Vietcombank phát hành mang các thương hiệu Visa, Mastercard, Amex, JCB còn hiệu lực.
Khách hàng tổ chức là chủ thẻ tín dụng công ty do VCB phát hành mang các thương hiệu Visa và Amex còn hiệu lực.

</td>
</tr>
</table>

		3. <u>Đăng ký 3D-SECURE như thế nào?</u> *Để được bảo vệ bởi 3D-SECURE, Khách hàng cần đăng ký **Số điện thoại** để nhận mật khẩu giao dịch một lần (OTP) khi giao dịch trực tuyến.* – Với các Khách hàng đã đăng ký số điện thoại nhận OTP từ trước, Vietcombank sẽ tự động gửi mật khẩu giao dịch vào số điện thoại đó (Khách hàng không phải đăng ký lại). – Với các Khách hàng chưa đăng ký: Quý Khách có thể đăng ký trên VCB Digibank trên trình duyệt web hoặc tại các điểm giao dịch của Vietcombank. **4. <u>Làm thế nào để sử dụng 3D-SECURE khi thanh toán trực tuyến?</u>** *Sau khi đăng ký, Khách hàng sẽ được bởi vệ bởi 3D-SECURE khi thanh toán trực tuyến, cụ thể như sau:* – **Bước 1**: Khách hàng chọn hàng hóa dịch vụ từ website trực tuyến có biểu tượng 3D-SECURE. – **Bước 2**: Nhập các thông tin thanh toán theo yêu cầu. – **Bước 3**: Lựa chọn hình thức nhận mật khẩu xác thực giao dịch qua SMS/email. – **Bước 4**: Nhập mật khẩu xác thực giao dịch được cung cấp bởi Vietcombank. – **Bước 5**: Giao dịch sẽ được tiếp tục xử lý và hoàn tất.