Payoo

CẨM NANG AN TOÀN BẢO MẬT

khi sử dụng dịch vụ thanh toán trực tuyến Payoo

Kính gửi Quý Khách hàng

Payoo luôn chú trọng bảo vệ thông tin và tài sản của Quý Khách hàng. Trước sự gia tăng của các hình thức gian lận ngày càng tinh vi, cẩm nang này mang đến những hướng dẫn thiết thực để Quý Khách hàng chủ động bảo vệ tài khoản và giao dịch của mình một cách an toàn.

1. BẢO MẬT TÀI KHOẢN

1.1 Bảo vệ mật khẩu, mã PIN và mã OTP

Mật khẩu, mã PIN và mã OTP là “chìa khóa” để truy cập tài khoản của bạn. Nếu những thông tin này bị lộ, tài khoản có thể bị chiếm quyền, bị đánh cắp thông tin và phát sinh giao dịch trái phép chỉ trong thời gian ngắn.

Lời khuyên từ Payoo:

- Tuyệt đối giữ bí mật mật khẩu, mã PIN và mã OTP. Không chia sẻ với bất kỳ ai, kể cả người thân hoặc người tự xưng là nhân viên ngân hàng / Payoo.
- Không chụp màn hình hoặc gửi mã OTP qua tin nhắn, email hoặc mạng xã hội dưới bất kỳ hình thức nào.
- Không lưu mật khẩu hoặc mã PIN trong ghi chú điện thoại, email hoặc tin nhắn vì đây là những nơi dễ bị truy cập trái phép.
- Luôn bảo vệ thiết bị nhận OTP (điện thoại, ứng dụng Payoo...). Không cho người khác mượn hoặc sử dụng thiết bị đã đăng ký nhận OTP của bạn.

Payoo không bao giờ yêu cầu Quý Khách hàng cung cấp mật khẩu hoặc mã OTP qua điện thoại, email, tin nhắn hoặc bất kỳ kênh nào khác. Mọi yêu cầu như vậy đều là dấu hiệu lừa đảo.

1.2 Thiết lập mật khẩu mạnh và thay đổi định kỳ

Mật khẩu mạnh giống như một “lớp khiên” giúp bảo vệ tài khoản và giảm nguy cơ bị truy cập trái phép.

Nguyên tắc đặt mật khẩu an toàn:

✓ NÊN	✗ KHÔNG NÊN
✓ Tối thiểu 8 ký tự, khuyến khích 12 ký tự trở lên. Kết hợp chữ hoa, chữ thường, số và ký tự đặc biệt (@, #, !)	✗ Sử dụng các dãy số/chữ đơn giản: 123456, abcdef, password, 111111
✓ Sử dụng cụm từ dễ nhớ nhưng khó đoán (ví dụ: một câu viết tắt hoặc đặc điểm cá nhân)	✗ Sử dụng thông tin cá nhân dễ đoán: ngày sinh, số điện thoại, biển số xe, tên người thân để đặt mật khẩu
✓ Thay đổi mật khẩu định kỳ ít nhất 6 tháng/lần	✗ Giữ nguyên mật khẩu mặc định được cấp lần đầu
✓ Đặt mã PIN giao dịch khác mật khẩu đăng nhập	✗ Dùng chung một mật khẩu cho nhiều tài khoản (email, mạng xã hội)

Mẹo tạo mật khẩu mạnh và dễ nhớ: Chọn một câu có ý nghĩa với bạn, lấy chữ cái đầu mỗi từ, thêm số và ký tự đặc biệt. Ví dụ: "Tôi thích uống Cà Phê mỗi buổi Sáng" → Ttu#CaPhe@mbS! (14 ký tự)

1.3. Không lưu thông tin đăng nhập trên trình duyệt

Các trình duyệt như Chrome, Safari, Edge hoặc Firefox thường đề xuất lưu tên đăng nhập và mật khẩu để tiện sử dụng. Tuy nhiên, điều này có thể làm tăng rủi ro lộ thông tin nếu thiết bị bị mất, bị xâm nhập hoặc có người khác sử dụng.

Lời khuyên từ Payoo:

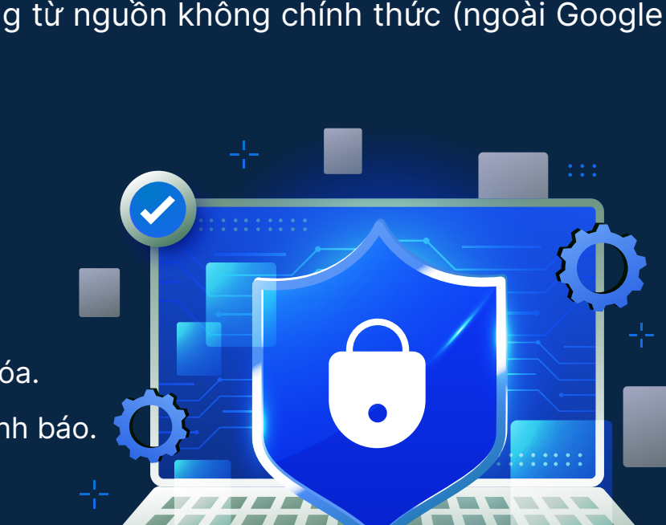
- Từ chối lưu mật khẩu khi trình duyệt hiển thị thông báo “Bạn có muốn lưu mật khẩu không?”
- Thường xuyên kiểm tra và xóa các mật khẩu đã lưu trong phần cài đặt (Settings ⇒ Passwords / Mật khẩu đã lưu).
- Không sử dụng các tùy chọn như “Ghi nhớ đăng nhập” hoặc “Duy trì đăng nhập” đối với các dịch vụ liên quan đến thanh toán.
- Không lưu thông tin thẻ ngân hàng trên các website hoặc nền tảng mua sắm không đáng tin cậy.

1.4. Đăng xuất khi không sử dụng

Việc quên đăng xuất khỏi ứng dụng hoặc website thanh toán có thể tạo cơ hội cho người khác truy cập vào tài khoản, nhất là khi sử dụng thiết bị chung hoặc khi điện thoại không được khóa màn hình.

Lời khuyên từ Payoo:

- Luôn đăng xuất (log out) khỏi ứng dụng Payoo và các dịch vụ thanh toán trực tuyến ngay sau khi hoàn tất giao dịch.
- Thiết lập khóa màn hình tự động trên điện thoại bằng mã PIN, vân tay hoặc nhận diện khuôn mặt, với thời gian khóa ngắn (khoảng 30 giây – 1 phút).
- Không để thiết bị ở trạng thái đã đăng nhập sẵn khi rời đi, kể cả trong thời gian ngắn.



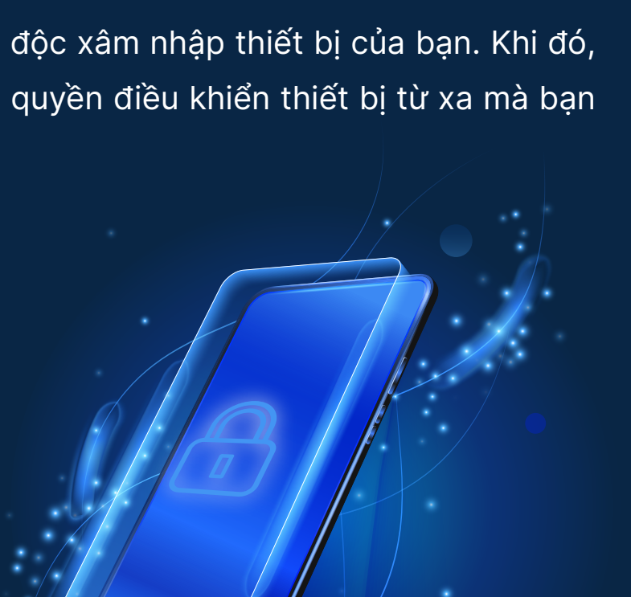
2. THÔNG TIN AN TOÀN THIẾT BỊ

2.1. Sử dụng thiết bị di động an toàn

Không sử dụng thiết bị đã can thiệp hệ thống (Root hoặc Jailbreak). Root (Android) và Jailbreak (iOS) là việc can thiệp vào hệ điều hành, làm mất các lớp bảo vệ mặc định. Điều này cho phép cài đặt ứng dụng từ nguồn không chính thức (ngoài Google Play, App Store) và truy cập sâu vào hệ thống thiết bị.

Rủi ro có thể xảy ra:

- Mã độc dễ dàng xâm nhập và chiếm quyền kiểm soát thiết bị.
- Các cơ chế bảo mật tích hợp của ứng dụng ngân hàng và thanh toán có thể bị vô hiệu hóa.
- Dữ liệu nhạy cảm (mật khẩu, thông tin thẻ, mã OTP) có thể bị đánh cắp mà không có cảnh báo.



Lời khuyên từ Payoo:

- Tuyệt đối không sử dụng thiết bị đã Root/Jailbreak để cài đặt và sử dụng ứng dụng thanh toán, tài chính, ngân hàng hoặc ứng dụng tạo OTP.
- Nếu thiết bị đã bị Root/Jailbreak, hãy khôi phục về trạng thái cài đặt gốc (factory reset) trước khi sử dụng. Lưu ý: thao tác này sẽ xóa toàn bộ dữ liệu trên thiết bị, bạn cần sao lưu trước khi thực hiện.
- Khi mua thiết bị cũ, cần kiểm tra xem thiết bị có bị Root/Jailbreak hay không trước khi dùng cho các giao dịch tài chính.

2.2. Cập nhật phần mềm và bảo vệ thiết bị

Lỗ hổng bảo mật trong hệ điều hành và ứng dụng có thể trở thành "cánh cửa" để mã độc xâm nhập thiết bị của bạn. Khi đó, kẻ gian có thể theo dõi thao tác, đánh cắp thông tin đăng nhập hoặc thậm chí chiếm quyền điều khiển thiết bị từ xa mà bạn không hay biết.

Lời khuyên từ Payoo:

- Cập nhật hệ điều hành (iOS, Android) lên phiên bản mới nhất ngay khi có thông báo.
- Cập nhật ứng dụng Payoo và các ứng dụng ngân hàng lên phiên bản mới nhất trên App Store hoặc Google Play.
- Bật tính năng cập nhật tự động (auto-update) cho hệ điều hành và ứng dụng để không bỏ lỡ các cập nhật bảo mật quan trọng.
- Bảo vệ thiết bị trước mã độc:

Trên Android: Cài đặt phần mềm bảo mật (diệt virus/chống mã độc) đáng tin cậy và cập nhật thường xuyên để bảo vệ thiết bị trước virus và mã độc mới.

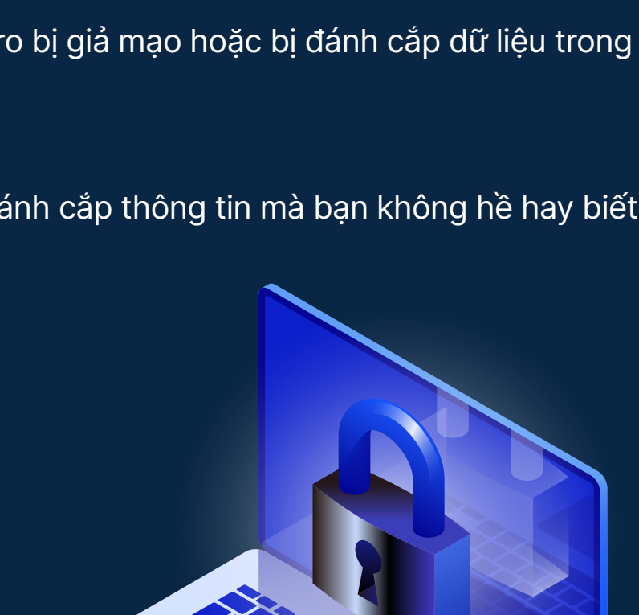
Trên iPhone (iOS): Luôn cập nhật iOS lên phiên bản mới nhất — đây là biện pháp bảo vệ hiệu quả nhất do Apple đã tích hợp sẵn các cơ chế bảo mật trong hệ điều hành.

2.3. Không cài đặt phần mềm lạ, không bản quyền hoặc không rõ nguồn gốc

Phần mềm không rõ nguồn gốc là một trong những con đường phổ biến nhất để mã độc xâm nhập thiết bị. Nhiều ứng dụng "miễn phí" hoặc bị "bẻ khóa" (crack) đã được cài sẵn mã độc để đánh cắp thông tin hoặc kiểm soát thiết bị từ xa.

Lời khuyên từ Payoo:

- Chỉ cài đặt ứng dụng từ các kho ứng dụng chính thức như: App Store (iOS) và Google Play (Android).
- Không tải phần mềm từ các trang web không chính thức, đường link chia sẻ trên mạng xã hội hoặc file đính kèm trong email/tin nhắn.
- Không cài đặt phần mềm bẻ khóa (crack/keygen), hoặc phần mềm không có bản quyền.
- Kiểm tra quyền truy cập (permissions) mà ứng dụng yêu cầu trước khi cài đặt. Cảnh giác với các ứng dụng yêu cầu quá nhiều quyền không liên quan đến chức năng của chúng (ví dụ: ứng dụng đèn pin yêu cầu quyền đọc tin nhắn hoặc quản lý cuộc gọi).
- Đặc biệt không cấp quyền Trợ năng (Accessibility) cho các ứng dụng không đáng tin cậy. Đây là quyền có thể cho phép ứng dụng đọc và điều khiển toàn bộ thao tác trên màn hình.



Quét mã QR để tải ứng dụng

2.4. Hạn chế sử dụng máy tính và mạng WiFi công cộng

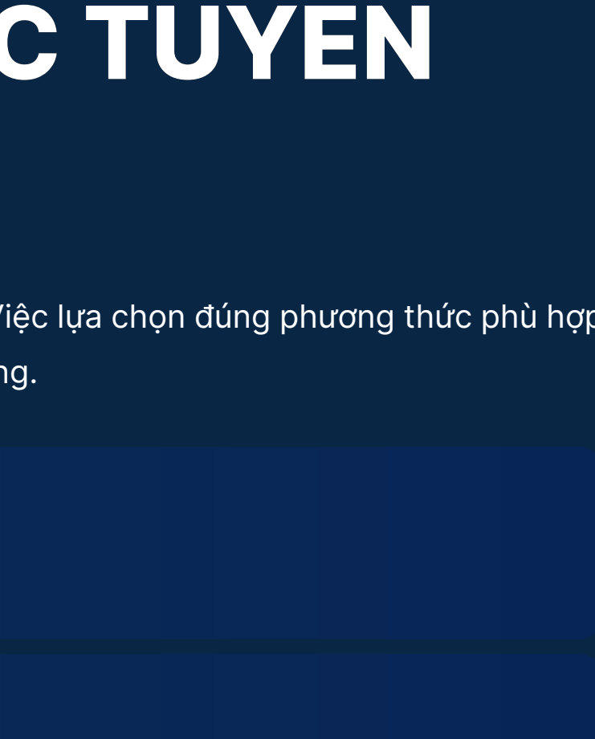
Máy tính tại quán Internet, thư viện, sân bay hoặc khách sạn có nguy cơ bị cài phần mềm theo dõi (keylogger), ghi lại toàn bộ thao tác bàn phím – bao gồm cả thông tin đăng nhập của bạn.

Tương tự, WiFi công cộng (quán cà phê, trung tâm thương mại, sân bay...) tiềm ẩn rủi ro bị giả mạo hoặc bị đánh cắp dữ liệu trong quá trình truyền tải thông tin.

Kẻ gian cũng có thể tạo các mạng WiFi giả với tên giống địa điểm bạn đang ở nhằm đánh cắp thông tin mà bạn không hề hay biết.

Lời khuyên từ Payoo:

- Tránh sử dụng máy tính công cộng hoặc thiết bị của người khác để đăng nhập tài khoản thanh toán. Nếu đã đăng nhập trên thiết bị không phải của mình, hãy đăng xuất ngay sau khi sử dụng, đồng thời xóa lịch sử trình duyệt và dữ liệu đã lưu.
- Không thực hiện giao dịch tài chính khi sử dụng WiFi công cộng hoặc WiFi miễn phí. Nên chuyển sang kết nối 4G/5G từ nhà mạng di động. Trong trường hợp bắt buộc phải sử dụng wifi công cộng, nên sử dụng VPN (ứng dụng giúp bảo mật kết nối) đáng tin cậy để mã hóa và bảo vệ dữ liệu.



3. AN TOÀN
TRONG GIAO DỊCH TRỰC TUYẾN

3.1. Lựa chọn hình thức xác nhận giao dịch phù hợp

Payoo cung cấp nhiều hình thức xác nhận giao dịch với mức độ bảo mật khác nhau. Việc lựa chọn đúng phương thức phù hợp sẽ giúp bạn cân bằng giữa tiện lợi và an toàn, đặc biệt đối với các giao dịch quan trọng.

CƠ BẢN ✓ — — —	**MẬT KHẨU**	Tra cứu thông tin, giao dịch giá trị nhỏ
TRUNG BÌNH ✓ ✓ — —	**MÃ OTP QUA SMS**	Giao dịch thông thường
CAO ✓ ✓ ✓ —	**MÃ OTP QUA ỨNG DỤNG SINH OTP (SOFT OTP/SMARTOTP)**	Giao dịch giá trị lớn
RẤT CAO ✓ ✓ ✓ ✓	**XÁC THỰC SINH TRẮC HỌC (VÂN TAY, KHUÔN MẶT)**	Giao dịch giá trị lớn, thay đổi thông tin quan trọng/thông tin định danh tài khoản

Hướng dẫn lựa chọn:

- Thiết lập hạn mức giao dịch phù hợp với nhu cầu sử dụng thực tế. Không nên đặt hạn mức quá cao để giảm thiểu rủi ro khi tài khoản bị xâm phạm.
- Luôn bật xác thực hai yếu tố (2FA) để tăng cường bảo mật cho tài khoản.
- Đối với các giao dịch có giá trị lớn hoặc giao dịch quan trọng, hãy ưu tiên sử dụng OTP qua ứng dụng hoặc xác thực sinh trắc học thay vì chỉ dùng mật khẩu hoặc SMS OTP.
- Để thay đổi hình thức xác nhận giao dịch, vào Cài đặt → Bảo mật trong ứng dụng Payoo hoặc liên hệ tổng đài 1900 54 54 78 để được hỗ trợ.

3.2. Cảnh báo rủi ro khi sử dụng dịch vụ thanh toán trực tuyến

Thanh toán trực tuyến mang lại nhiều tiện ích. Tuy nhiên, để đảm bảo an toàn khi giao dịch, người dùng cần trang bị các kiến thức và biện pháp phòng tránh rủi ro.

RỦI RO	HẬU QUẢ	BIỆN PHÁP PHÒNG TRÁNH
Bị đánh cắp thông tin qua phần mềm gián điệp, trang web giả mạo, hoặc các hình thức lừa đảo.	Mất quyền kiểm soát tài khoản	Xem mục 1.1, 3.3
Lộ thông tin đăng nhập dẫn đến các giao dịch trái phép	Mất tiền trong tài khoản	Xem mục 1.2, 3.1
Thiết bị bị nhiễm mã độc hoặc bị truy cập trái phép	Mã độc đánh cắp mật khẩu, mã OTP từ xa	Xem mục 2.1, 2.2, 2.3
Mạng kết nối không an toàn, dữ liệu giao dịch bị nghe lén	Lộ thông tin giao dịch, và đăng nhập	Xem mục 2.4
Chia sẻ thông tin với bên thứ ba không đáng tin cậy	Rò rỉ dữ liệu cá nhân và tài khoản	Xem mục 1.1, 1.3

ĐỂ GIẢM THIỂU RỦI RO, PAYOO KHUYẾN NGHỊ:

- **Bật thông báo giao dịch** qua ứng dụng hoặc SMS để phát hiện kịp thời mọi hoạt động trên tài khoản, đặc biệt là các dịch vụ tài chính cần theo dõi biến động số dư.
- **Kiểm tra sao kê định kỳ** (ít nhất mỗi tuần) để phát hiện giao dịch bất thường.
- **Thiết lập hạn mức giao dịch** phù hợp nhu cầu thực tế. Hạn mức thấp hơn giúp giảm thiệt hại nếu tài khoản bị xâm phạm.
- **Không chia sẻ thông tin tài khoản** với bất kỳ ứng dụng hoặc dịch vụ bên thứ ba nào không được Payoo chính thức hỗ trợ.

Payoo liên tục nâng cấp hệ thống bảo mật và giám sát giao dịch 24/7 để bảo vệ Quý Khách hàng. Tuy nhiên, sự chủ động phòng tránh từ phía khách hàng là yếu tố quan trọng nhất để đảm bảo an toàn.

3.3. Nhận diện và phòng tránh lừa đảo trực tuyến

Các hình thức lừa đảo ngày càng tinh vi, sử dụng nhiều chiêu thức để đánh cắp thông tin và tài sản của bạn. Dưới đây là một số hình thức lừa đảo phổ biến và cách nhận biết.

	CÁCH NHẬN BIẾT	CÁCH PHÒNG TRÁNH
Giả mạo trang web (Phishing)	• Đường link được gửi qua email, SMS hoặc mạng xã hội yêu cầu đăng nhập tài khoản • Tên miền gần giống nhưng bị biến thể, thay đổi ký tự (ví dụ: pay0o.vn, payoo-vn.com...) • Không có **https://** hoặc thiếu biểu tượng ổ khóa trên thanh địa chỉ. • Giao diện giống Payoo nhưng có các dấu hiệu bất thường	• Không đăng nhập vào các trang web từ các đường link lạ • Chỉ truy cập website chính thức: **payoo.vn** hoặc **payoo.com.vn**
Giả mạo ứng dụng	• Đường Link tải trực tiếp ứng dụng, file .apk trên android được gửi qua tin nhắn, email, mạng xã hội của bạn • Thông tin nhà phát triển không rõ ràng, ít đánh giá hoặc có dấu hiệu bất thường • Yêu cầu các quyền truy cập không cần thiết	• Chỉ tải ứng dụng từ **App Store** hoặc **Google Play** • Kiểm tra tên nhà phát triển, số lượt tải và đánh giá trước khi cài đặt • Gỡ bỏ ngay nếu phát hiện ứng dụng đáng ngờ
Giả danh nhân viên hỗ trợ	• Kẻ gian chủ động gọi điện hoặc nhắn tin, tự xưng là nhân viên Payoo, ngân hàng hoặc cơ quan chức năng • Yêu cầu cung cấp **mật khẩu, mã OTP, thông tin cá nhân** hoặc cài đặt ứng dụng lạ • Tạo áp lực với các lý do như: “tài khoản gặp sự cố”, “cần xử lý gấp”,...	• Không cung cấp bất kỳ thông tin cá nhân nào qua điện thoại hoặc tin nhắn • Không nhấn vào đường link hoặc tải ứng dụng theo hướng dẫn của người lạ • Chủ động liên hệ tổng đài chính thức của Payoo: **1900 54 54 78** để xác minh
Lừa đảo trúng thưởng, khuyến mãi giả	• Nhận được thông báo trúng thưởng bất ngờ • Yêu cầu chuyển “phí nhận thưởng” hoặc cung cấp thông tin tài khoản • Thông tin không xuất hiện trên các kênh chính thức của nhà cung cấp dịch vụ. Luôn kiểm chứng lại thông tin từ nguồn độc lập	• Không chuyển tiền dưới bất kỳ hình thức nào. **Payoo không bao giờ** yêu cầu khách hàng chuyển tiền để nhận quà tặng hoặc khuyến mãi • Không cung cấp thông tin cá nhân • Kiểm tra chương trình trên website hoặc kênh chính thức của Payoo
Tin nhắn giả mạo (Smishing)	• Tin nhắn có nội dung khẩn cấp như: “tài khoản bị khóa”, “giao dịch đáng ngờ cần xác minh” • Có kèm đường link lạ yêu cầu đăng nhập • Tên hiển thị (brandname) giống Payoo hoặc ngân hàng	• Không nhấn vào đường link trong tin nhắn. **Payoo không bao giờ** gửi tin nhắn SMS chứa đường link yêu cầu đăng nhập • Mở trực tiếp ứng dụng Payoo trên điện thoại để kiểm tra
Mã QR giả mạo	• Mã QR được gửi từ nguồn không xác minh được (tờ rơi lạ, tin nhắn từ người không quen, dán nơi công cộng) • Mã QR tại quầy thanh toán có dấu hiệu bị dán đè hoặc thay thế • Thông tin người nhận hiển thị không rõ ràng	• Không quét mã QR từ các nguồn không xác minh được • Kiểm tra kỹ thông tin người nhận tiền hiển thị trên màn hình trước khi xác nhận thanh toán

3.4. Xử lý ngay khi phát hiện giao dịch bất thường

Thời gian phản ứng là yếu tố quan trọng khi tài khoản có dấu hiệu bị xâm phạm. Chỉ một vài phút chậm trễ cũng có thể khiến thiệt hại gia tăng.

Các dấu hiệu giao dịch bất thường:

- Nhận được thông báo giao dịch mà bạn không thực hiện.
- Số dư tài khoản thay đổi bất thường.
- Nhận được mã OTP khi bạn không yêu cầu.
- Phát hiện đăng nhập từ thiết bị hoặc vị trí không quen thuộc.
- Thông tin tài khoản (email, số điện thoại liên kết) bị thay đổi mà bạn không thực hiện.

Khi phát hiện dấu hiệu bất thường, hãy thực hiện ngay:

1. Khóa tài khoản/thẻ ngay lập tức thông qua ứng dụng (nếu có tính năng).
2. Đổi mật khẩu tài khoản.
3. Liên hệ Payoo qua tổng đài 1900 54 54 78 hoặc email: support@payoo.vn để được hỗ trợ.
4. Liên hệ ngân hàng phát hành thẻ để khóa thẻ nếu cần

3.5. Thông báo ngay khi mất thiết bị hoặc bị lừa đảo

Trong các tình huống khẩn cấp, việc thông báo kịp thời sẽ giúp hạn chế tối đa rủi ro và bảo vệ tài khoản của bạn.

TÌNH HUỐNG	HÀNH ĐỘNG CẦN LÀM NGAY
Mất, thất lạc hoặc hư hỏng điện thoại đã đăng ký nhận OTP	Gọi tổng đài 1900 54 54 78 yêu cầu tạm khóa tài khoản; liên hệ nhà mạng khóa SIM
Mất hoặc hư hỏng thiết bị tạo OTP (Soft OTP, Smart OTP)	Gọi tổng đài yêu cầu vô hiệu hóa OTP cũ và thiết lập lại phương thức xác thực.
Mất số điện thoại nhận tin nhắn SMS xác thực	Liên hệ nhà mạng để khóa/khôi phục SIM; thông báo Payoo để cập nhật số mới
Mất hoặc hư hỏng thiết bị lưu trữ khóa bảo mật/chữ ký điện tử	Gọi tổng đài yêu cầu thu hồi khóa cũ và cấp khóa mới
Bị lừa đảo hoặc nghi ngờ bị lừa đảo (đã cung cấp thông tin cho kẻ gian)	Gọi tổng đài khóa tài khoản ngay; đổi mật khẩu; trình báo cơ quan công an
Bị tấn công mạng hoặc nghi ngờ thiết bị bị kiểm soát từ xa	Ngắt kết nối Internet trên thiết bị; gọi tổng đài Payoo để khóa/tạm khóa tài khoản và hỗ trợ xử lý; khôi phục cài đặt gốc thiết bị sau khi đã sao lưu dữ liệu quan trọng

5 NGUYÊN TẮC VÀNG

BẢO VỆ TÀI KHOẢN

1. **BÍ MẬT** Không chia sẻ mật khẩu, mã PIN, mã OTP với bất kỳ ai
2. **CẢNH GIÁC** Không nhấn link lạ, không quét QR lạ, không tải ứng dụng ngoài kho chính thức, không tin lời mời trúng thưởng
3. **CẬP NHẬT** Luôn cập nhật hệ điều hành, ứng dụng và phần mềm bảo mật lên phiên bản mới nhất
4. **AN TOÀN** Không dùng WiFi công cộng, không dùng thiết bị Root/Jailbreak, không lưu mật khẩu trên trình duyệt khi đăng nhập và thực hiện giao dịch tài chính
5. **NHANH CHÓNG** Khi phát hiện bất thường, liên hệ Payoo ngay qua tổng đài 1900 54 54 78

THÔNG TIN LIÊN HỆ

☎ Tổng đài hỗ trợ: 1900 54 54 78
✉ Email: support@payoo.vn
Website: payoo.vn

TẢI ỨNG DỤNG CHÍNH THỨC

Quét mã QR để tải ứng dụng

Cùng Payoo bảo vệ tài khoản của bạn — An toàn giao dịch, An tâm sử dụng