

TÀI LIỆU TRUYỀN THÔNG CỘNG ĐỒNG

BỘ NGUYÊN TẮC NHẬN DIỆN VÀ PHÒNG, CHỐNG LỪA ĐẢO TRỰC TUYẾN



Dành cho cộng đồng · Đọc trong 10 phút · Dùng được cả đời

CHẬM LẠI · KIỂM TRA · XÁC MINH
KHÔNG CHUYỂN TIẾN · BÁO CÁO

MỤC LỤC

Trong sổ tay này có gì

	Bộ 10 dấu hiệu nhận biết lừa đảo	4
	Bộ 10 nguyên tắc phòng, chống lừa đảo	5
	Các tình huống điển hình	6
	Xử lý trong 30 phút đầu	10
	Danh bạ khẩn cấp	13
	Giữ mình mỗi tháng 5 phút	14

CHẬM LẠI – KIỂM TRA – XÁC MINH
KHÔNG CHUYỂN TIỀN – BÁO CÁO

**Kẻ lừa đảo không tấn công điện thoại của bạn.
Chúng tấn công cảm xúc của bạn.**

Trước mọi lần chuyển tiền, hãy hỏi 3 câu:

- 1. Ai đang hỏi thúc tôi, và vì sao phải gấp đến vậy?**
- 2. Tôi có tự kiểm chứng được qua kênh chính thức không?**
- 3. Nếu dừng lại 1 tiếng, tôi mất gì? (Gần như luôn là: không mất gì.)**

CÔNG CỤ NÊN CÓ SẴN TRÊN ĐIỆN THOẠI

ntrust.vn

Ứng dụng miễn phí: kiểm tra số điện thoại, số tài khoản, link, mã QR; chặn cuộc gọi lừa đảo

156 / 5656

Tổng đài miễn phí phản ánh cuộc gọi, tin nhắn lừa đảo

nospam.vncert.vn

Phản ánh tin nhắn rác, cuộc gọi rác và tin nhắn có dấu hiệu lừa đảo

chongluadao.vn

Kiểm tra website, đường link nghi ngờ và gửi báo cáo vụ việc lừa đảo

tracnghiem.chongluadao.vn

Làm trắc nghiệm tự kiểm tra kỹ năng nhận diện lừa đảo

baovethongtin.com

Checklist hướng dẫn bảo mật thông tin

1. Bộ 10 dấu hiệu nhận biết lừa đảo

1 dấu hiệu → dừng lại và kiểm chứng · 2 dấu hiệu → gần như chắc chắn lừa đảo.

NHÓM A · ÉP CẢM XÚC



01 Tạo cảm giác khẩn cấp

"Làm ngay trong 30 phút, không thì mất tiền"



02 Đe dọa, gây hoảng sợ

Dọa liên quan án hình sự, sắp bị bắt, bị phạt



03 Yêu cầu giữ bí mật

Ép ra chỗ vắng, cấm kể cho người thân

NHÓM B · ĐÒI THÔNG TIN & QUYỀN



04 Đòi mật khẩu, OTP, mã xác thực

Kể cả người xưng nhân viên ngân hàng, công an



05 Yêu cầu chuyển tiền trước

Phí xác minh, tiền cọc, "chứng minh tài chính"



06 Bắt cài ứng dụng không rõ nguồn gốc

File .apk, link lạ ngoài CH Play / App Store



07 Đòi chia sẻ màn hình, điều khiển từ xa

Quyền Trợ năng, TeamViewer, UltraViewer

NHÓM C · LINK, QR, TẠO LÒNG TIN



08 Gửi link hoặc mã QR đáng ngờ

Tên miền sai chính tả, QR dán đè lên QR gốc



09 Hứa lợi nhuận, quà tặng bất thường

"Việc nhẹ lương cao", "lãi cao không rủi ro"



10 Giả danh cơ quan, lãnh đạo, người thân

Tài khoản nhận tiền lại mang tên người lạ

2. Bộ 10 nguyên tắc phòng, chống lừa đảo

Chậm lại · Kiểm tra · Xác minh · Không chuyển tiền · Báo cáo



01 DỪNG 10 GIÂY

Không quyết định tiền bạc khi đang bị hối thúc



02 3 KHÔNG

Không link lạ – Không QR lạ – Không app lạ



03 OTP LÀ CỦA RIÊNG BẠN

Không đưa OTP, mật khẩu, khuôn mặt cho bất kỳ ai



04 CHƯA XÁC MINH – CHƯA CHUYỂN

Kiểm tra kỹ tên người nhận trước khi bấm xác nhận



05 TỰ TRẢ SỐ, TỰ GỌI LẠI

Không gọi số do người lạ cung cấp



06 NGHE ĐƯỢC GIỌNG THẬT

Người thân vay tiền: gọi thoại thường, hỏi "mật khẩu gia đình"



07 CƠ QUAN CHÚC NẮNG KHÔNG GỌI ĐÒI TIỀN

Chỉ mời làm việc tại trụ sở, không có "tài khoản tạm giữ"



08 KHÔNG NẠP TIỀN TRƯỚC

Không có việc làm hay khoản đầu tư nào bắt nạp trước



09 KHÓA CỬA NHÀ MÌNH

Bật 2FA, đặt hạn mức chuyển tiền, cập nhật phần mềm



10 GIỮ BẰNG CHỨNG & BÁO NGAY

Ngân hàng → Công an → 156 → chongluadao.vn

IN RA VÀ DÁN LÊN

Dán bộ nguyên tắc này cạnh điện thoại bàn hoặc cửa tủ lạnh. Người cao tuổi trong gia đình nên có một bản riêng in cỡ chữ lớn.

3. Các tình huống điển hình

1. Giả danh công an, cơ quan chức năng

Kịch bản	Gọi điện đọc đúng thông tin cá nhân, dọa liên quan đường dây ma túy/rửa tiền, ép chuyển tiền vào "tài khoản tạm giữ" hoặc cài "app Bộ Công an" giả.
Dấu hiệu	Dọa nạt, ép ra chỗ vắng, cấm kể người thân, đòi tiền hoặc đòi cài app.
Sai lầm	Hoảng sợ, làm theo để "chứng minh mình trong sạch".
Xác minh	Công an chỉ mời làm việc tại trụ sở bằng giấy mời/giấy triệu tập. Không hề có "tài khoản tạm giữ".
Xử lý đúng	Dập máy, chặn số, không đổi co. Cần yên tâm thì gọi công an xã/phường nơi cư trú.

2. Giả danh người thân, lãnh đạo, đồng nghiệp

Kịch bản	Nick người thân hoặc sếp nhắn vay tiền gấp, hoặc yêu cầu chuyển khoản "việc gấp của công ty".
Dấu hiệu	Rất gấp; chỉ nhắn tin và né gọi thoại; tài khoản nhận tiền mang tên người lạ.
Sai lầm	Nể nang, chuyển trước hỏi sau.
Xác minh	Gọi thoại thường vào số đã lưu trong danh bạ. Doanh nghiệp phải xác minh hai kênh trước khi chi tiền.
Xử lý đúng	Chưa nghe được giọng thật thì chưa chuyển tiền. Tên người nhận không khớp → dừng ngay.

3. Giả mạo bằng giọng nói, hình ảnh, video deepfake

Kịch bản	Gọi video vài giây đúng mặt người thân rồi cúp vì "mạng yếu" và hỏi chuyển khoản; hoặc ghép mặt nạn nhân vào video nhạy cảm để tống tiền.
Dấu hiệu	Video ngắn, mờ, tiếng lệch khẩu hình, khuôn mặt thiếu cảm xúc, cử động không tự nhiên.
Sai lầm	Tin tuyệt đối vào "mắt thấy tai nghe".
Xác minh	Yêu cầu quay ngang mặt hoặc đứng dậy trước camera; hỏi "mặt khẩu gia đình"; gọi lại bằng cuộc gọi thoại thường.
Xử lý đúng	Không chuyển tiền. Bị tống tiền: không trả, không xóa bằng chứng, báo nền tảng và trình báo công an.

4. Lừa cài ứng dụng, chiếm quyền điều khiển điện thoại

Kịch bản	Giả cán bộ Thuế, BHXH, công an khu vực hỏi "cập nhật sinh trắc học, VNeID", gửi file .apk. App xin quyền Trợ năng rồi tự đọc OTP và rút sạch tiền.
Dấu hiệu	Link tải app gửi qua Zalo/SMS; app đòi quyền Trợ năng; máy nóng, hao pin bất thường.
Sai lầm	Thấy quốc huy hoặc logo ngân hàng nên cấp hết mọi quyền.
Xác minh	App chính thống chỉ có trên App Store và CH Play. Thủ tục định danh làm tại công an xã/phường.
Xử lý đúng	Bật chế độ máy bay → tắt quyền Trợ năng → gỡ app → khóa tài khoản → khôi phục cài đặt gốc.

5. Lừa đảo đầu tư, cộng tác viên, hoàn tiền

Kịch bản	Mời làm cộng tác viên hoặc đầu tư qua app lạ. Vài lần đầu cho rút lãi thật (tiền mới), sau đó "báo lỗi" và bắt nạp thêm để "giải cứu tiền gốc".
Dấu hiệu	Lợi nhuận phi lý; liên tục đòi nạp thêm để sửa lỗi; app không có trên chợ ứng dụng.
Sai lầm	Tiếc số tiền đã nạp nên vay mượn nạp thêm để gỡ.
Xác minh	Không nơi làm việc hợp pháp nào bắt người lao động nạp tiền vào tài khoản cá nhân.
Xử lý đúng	Cắt lỗ dứt khoát, dừng nạp, lưu bằng chứng và trình báo. Không tin "dịch vụ lấy lại tiền".

6. Bắt cóc trực tuyến ("bắt cóc online")

Kịch bản	Giả danh công an, gọi cho học sinh, sinh viên, dọa em liên quan đường dây tội phạm kèm "lệnh bắt" giả. Chúng ép em rời nhà đến nhà nghỉ, cắt liên lạc với gia đình, tự quay video như đang bị giam giữ, rồi gọi cho cha mẹ đòi tiền chuộc. Nạn nhân hầu hết ở tuổi 18–22.
Dấu hiệu	Con em mất liên lạc đột ngột; đòi tiền chuộc trong 10–15 phút và cấm báo công an; ảnh, video, giọng nói có dấu hiệu cắt ghép; tài khoản nhận tiền tên người lạ.
Sai lầm	Chuyển tiền ngay vì quá sợ, và không dám báo công an đúng như lời đe dọa của kẻ gian.
Xác minh	Gọi ngay nhà trường, bạn cùng lớp, bạn cùng phòng để xác minh vị trí thật của em. Công an không yêu cầu người dân rời nhà đến nhà nghỉ hay cắt liên lạc với gia đình.
Xử lý đúng	Không chuyển tiền. Báo Công an xã/phường ngay – nhiều vụ đã giải cứu được trong vài giờ nhờ trình báo sớm. Gia đình nên thống nhất "mặt khẩu gia đình" và bật chia sẻ vị trí.

7. Giả danh shipper giao hàng

Kịch bản

Kẻ gian lấy tên, số điện thoại, địa chỉ và đơn hàng từ bình luận công khai dưới livestream bán hàng. Chúng gọi tự xưng shipper, nói đang giao gấp và để hàng ở cổng, xin chuyển khoản trước. Sau khi nhận tiền, chúng báo bạn "gửi nhầm số tài khoản" hoặc đã vô tình đăng ký "tài khoản chạy shipper", rồi đưa số tổng đài giả để dẫn dắt bạn chuyển thêm.

Dấu hiệu

Hối chuyển khoản khi bạn chưa nhận được hàng; tài khoản nhận tên cá nhân lạ; xuất hiện chuỗi "hủy đăng ký – hoàn tiền – sai cú pháp"; được cấp số tổng đài và link lạ.

Sai lầm

Chuyển khoản theo trí nhớ về đơn đã đặt; nhập "mã xác nhận hoàn tiền" vào app ngân hàng – thực chất là xác nhận một lệnh chuyển tiền đi.

Xác minh

Đối chiếu đơn hàng trong ứng dụng sàn thương mại điện tử. Tra số tổng đài đơn vị vận chuyển trên website chính thức, không gọi số do người lạ cung cấp.

Xử lý đúng

Chỉ trả tiền khi đã nhận và kiểm tra được hàng. Không có "hoàn tiền bằng cách chuyển thêm tiền". Không để lại số điện thoại, địa chỉ trong bình luận công khai. Đã chuyển thì xử lý theo Mục 2.4.

4 Xử lý trong 30 phút đầu



TUYỆT ĐỐI KHÔNG



Không chuyển thêm tiền

để “giải cứu tiền gốc”



**Không tin dịch vụ
“lấy lại tiền bị lừa” trên mạng**

Đó là lừa đảo vòng 2

Báo càng sớm, khả năng ngân hàng chặn được dòng tiền càng cao.

Đã bấm vào link giả

0-5 phút: Dóng trình duyệt, không điền bất kỳ thông tin gì; xóa file vừa tự tải về.

Trong 30 phút: Nếu đã lỡ điền: dùng máy khác đổi mật khẩu, bật 2FA, gọi ngân hàng khóa thẻ.

Đã cung cấp mật khẩu / OTP

0-5 phút: Gọi tổng đài ngân hàng khóa khẩn cấp tài khoản và thẻ.

Trong 30 phút: Đổi mật khẩu trên máy khác; đăng xuất mọi thiết bị; gỡ email/SĐT khôi phục lại.

Đã cài ứng dụng đáng ngờ

0-5 phút: Bật chế độ máy bay; tắt quyền Trợ năng của ứng dụng đó.

Trong 30 phút: Gỡ app (dùng Safe Mode nếu không gỡ được) → khóa tài khoản → khôi phục cài đặt gốc.

Đã chia sẻ màn hình / điều khiển từ xa

0-5 phút: Tắt nguồn máy hoặc ngắt Wifi/4G ngay lập tức.

Trong 30 phút: Mượn máy người thân khóa tài khoản, đổi mật khẩu, gỡ app điều khiển.

Đã chuyển tiền

0-5 phút: Gọi ngân hàng báo lừa đảo, yêu cầu tra soát và phong tỏa tài khoản nhận.

Trong 30 phút: Chụp toàn bộ bằng chứng → trình báo công an → phản ánh 156. Tuyệt đối không nạp thêm tiền.

Bị chiếm tài khoản MXH / ngân hàng

0–5 phút: Khóa tài khoản ngân hàng; báo nền tảng "tài khoản bị hack".

Trong 30 phút: Nhờ người thân đăng cảnh báo; đổi mật khẩu email trước tiên; bật 2FA.

TUYỆT ĐỐI KHÔNG

Không chuyển thêm tiền để "giải cứu tiền gốc". Không tin dịch vụ "lấy lại tiền bị lừa" trên mạng — đó là lừa đảo vòng 2.

KHI NGHI NGỜ HOẶC ĐÃ BỊ LỪA

5. Danh bạ khẩn cấp

Liên hệ theo thứ tự này

- 1 **Tổng đài ngân hàng**
Số in ở mặt sau thẻ – khóa tài khoản, tra soát, đề nghị phong tỏa tài khoản nhận
- 2 **Công an xã / phường gần nhất**
Trình báo và lập hồ sơ, mang theo CCCD và bằng chứng
- 3 **156 hoặc 5656**
Tổng đài miễn phí phản ánh cuộc gọi, tin nhắn lừa đảo
- 4 **chongluadao.vn**
Kiểm tra link và báo tin để cảnh báo cộng đồng

SỐ CẦN GHI SẴN – ĐIỂN VÀO ĐÂY

Tổng đài ngân hàng của tôi:

Công an xã/phường nơi tôi ở:

Người thân gọi khi cần xác minh:

MẪU TIN NHẮN 30 GIÂY GỬI NGÂN HÀNG / CÔNG AN

Tôi bị lừa chuyển khoản.

Thời gian: giờ ngày/...../.....

Số tiền: VNĐ

Đến tài khoản: Tên:

Ngân hàng nhận: SĐT đối tượng:

Đề nghị hỗ trợ tra soát và phong tỏa khẩn cấp.

PHÒNG NGỪA ĐỊNH KỲ

6. Giữ mình mỗi tháng 5 phút

- ☐ Bật xác thực 2 lớp cho email, Facebook/Zalo, ngân hàng
- ☐ Đặt hạn mức chuyển tiền mỗi ngày ở mức thấp phù hợp nhu cầu
- ☐ Bật thông báo biến động số dư cho mọi giao dịch
- ☐ Kiểm tra danh sách thiết bị đang đăng nhập, đăng xuất thiết bị lạ
- ☐ Cập nhật hệ điều hành và ứng dụng ngân hàng
- ☐ Rà lại quyền Trợ năng – chỉ giữ ứng dụng bạn thật sự cần
- ☐ Không lưu ảnh CCCD, mặt khẩu, mã thẻ trong thư viện ảnh hoặc ghi chú
- ☐ Nhắc lại "mặt khẩu gia đình" với người thân, đặc biệt người cao tuổi

LƯU Ý THEO TỪNG NHÓM

Người cao tuổi

Dán cạnh điện thoại: "Không ai được hỏi OTP. Cơ quan chức năng không gọi điện đòi tiền." Mọi yêu cầu tiền bạc phải gọi lại số đã lưu trong danh bạ mới thực hiện.

Học sinh – sinh viên

Không nhận "việc nhẹ lương cao"; không cho mượn CCCD hay tài khoản ngân hàng để "mở hộ" – có thể bị phong tỏa tài khoản và xử lý pháp luật.

Hộ kinh doanh online

Chỉ giao hàng khi tiền đã vào tài khoản thật; cảnh giác biên lai chuyển khoản đã chỉnh sửa; kiểm tra mã QR tại quầy hàng ngày.

Doanh nghiệp

Mọi lệnh chuyển tiền bất thường từ "sếp" qua email hay Zalo phải xác minh hai kênh – đây là chiêu giả mạo lãnh đạo, nay đã có deepfake giọng nói và hình ảnh.

SỔ TAY NHẬN DIỆN VÀ PHÒNG, CHỐNG LỪA ĐẢO TRỰC TUYẾN

Ghi nhận thực hiện

TẠP CHÍ ĐIỆN TỬ
AN NINH MẠNG VIỆT NAM
CƠ QUAN NGÔN LUẬN CỦA HIỆP HỘI AN NINH MẠNG QUỐC GIA

Chống
Lừa Đảo

ĐƠN VỊ THỰC HIỆN

Chống Lừa Đảo chongluadao.vn

Tạp chí An ninh mạng tapchianninhmang.vn

BIÊN TẬP

Ngô Minh Hiếu

Huỳnh Ngọc Khánh Minh

GIẤY PHÉP SỬ DỤNG

Creative Commons Ghi công – Phi thương mại – Chia sẻ tương tự 4.0 Quốc tế

CC BY-NC-SA 4.0

Bạn được tự do sao chép, in ấn và phát hành lại trên mọi phương tiện; được chỉnh sửa, chuyển thể, dịch và thiết kế lại – miễn phí và không cần xin phép, với ba điều kiện:

BY

Ghi công – Ghi rõ tên tác giả, đơn vị thực hiện và đường dẫn giấy phép; nêu rõ nếu bạn có chỉnh sửa.

NC

Phi thương mại – Không dùng sổ tay hoặc bản phái sinh cho mục đích thương mại.

SA

Chia sẻ tương tự – Bản chỉnh sửa hoặc phát triển thêm phải phát hành theo đúng giấy phép này.

DỪNG LẠI & LAN TỎA

Ghi công đúng, chia sẻ tự do

MIỄN TRỪ CHO MỤC ĐÍCH CỘNG ĐỒNG

Các cơ quan nhà nước, tổ chức giáo dục, ngân hàng và cơ quan báo chí được phép in ấn và đăng tải lại sổ tay này với mục đích phi lợi nhuận mà không cần xin phép riêng, miễn là giữ nguyên thông tin ghi công.

MẪU GHI CÔNG KHI SỬ DỤNG LẠI

Nguồn: Bộ nguyên tắc nhận diện và phòng, chống lừa đảo trực tuyến – Tạp chí điện tử An ninh mạng Việt Nam (tapchianninhmang.vn) và Chống Lừa Đảo (chongluadao.vn).
Phát hành theo giấy phép CC BY-NC-SA 4.0.

Toàn văn giấy phép: creativecommons.org/licenses/by-nc-sa/4.0

Sổ tay này được viết ra để lan tỏa. Rất mong bạn in, chiếu, đăng lại và chuyển thể cho tổ dân phố, nhà trường, cơ quan, doanh nghiệp của mình. Càng nhiều người đọc, càng ít người mất tiền.

Quyền tác giả đối với nội dung gốc thuộc về các đơn vị thực hiện. Gỡ bỏ thông tin ghi công hoặc phát hành lại dưới danh nghĩa khác là vi phạm giấy phép.

Phiên bản 1.0 · 2026 · Tài liệu phi lợi nhuận phục vụ cộng đồng

TẠP CHÍ ĐIỆN TỬ
AN NINH MẠNG VIỆT NAM
CƠ QUAN NGÔN LUẬN CỦA HIỆP HỘI AN NINH MẠNG QUỐC GIA

Chống
Lừa Đảo

TAPCHIANNINHMANH.VN - CHONGLUADAO.VN

Vì một không gian mạng an toàn