

BỘ TÀI CHÍNH
ỦY BAN CHỨNG KHOÁN NHÀ NƯỚC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 6486 /UBCK-CDS

Hà Nội, ngày 14 tháng 7 năm 2026

V/v tăng cường đảm bảo an ninh mạng và
phòng chống tội phạm sử dụng công nghệ cao
đối với hoạt động giao dịch chứng khoán trực
tuyến trên thị trường chứng khoán

Kính gửi:

Nhận ngày 17/7/2026

Nơi chuyển:

CT - HĐQT	
Tổng giám đốc	
GD Tài chính	
GD Nhân sự	
GD Đầu tư	
GD DVKH	
P.KT-LK	
P.Giao dịch	
P.Tư vấn	
P.Phân tích	
P.Đầu tư	
P.Hành chính	
P.Nhân sự	
P.Pháp chế	
P.IT	
P.KSGB	
CN TRHCM	
CN HN	

- Công ty chứng khoán;
- Công ty quản lý quỹ;
- Đại lý phân phối chứng chỉ quỹ.

Theo các cảnh báo của Công an thành phố Hà Nội trong thời gian vừa qua về việc bảo đảm an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao đối với hoạt động giao dịch chứng khoán điện tử có áp dụng xác thực sinh trắc học, đặc biệt là sự xuất hiện các phương thức, thủ đoạn mới của tội phạm sử dụng công nghệ cao nhằm can thiệp vào thiết bị đầu cuối, giả mạo dữ liệu sinh trắc học và lợi dụng sơ hở trong quy trình xác thực để chiếm đoạt tài sản. Vì vậy, để tăng cường công tác bảo đảm an ninh mạng, bảo vệ quyền và lợi ích hợp pháp của nhà đầu tư, góp phần bảo đảm thị trường chứng khoán hoạt động an toàn, công khai, minh bạch và ổn định, Ủy ban Chứng khoán Nhà nước đề nghị Quý Công ty khẩn trương nghiêm túc thực hiện các nội dung sau:

1. Tổ chức phổ biến, tuyên truyền về công tác bảo đảm an ninh mạng

- Phổ biến nội dung cảnh báo của Công an thành phố Hà Nội (chi tiết tại Phụ lục kèm theo) đến các đơn vị, bộ phận có liên quan, đặc biệt là các bộ phận Công nghệ thông tin, Pháp chế và nghiệp vụ.
- Tăng cường tuyên truyền, khuyến nghị nhà đầu tư nâng cao cảnh giác trước các phương thức, thủ đoạn lừa đảo trên không gian mạng; không cung cấp thông tin tài khoản, mã xác thực, dữ liệu sinh trắc học hoặc cài đặt ứng dụng không rõ nguồn gốc theo yêu cầu của các đối tượng giả mạo.
- Tổ chức nghiên cứu, phổ biến và triển khai thực hiện các quy định của pháp luật có hiệu lực từ ngày 01/7/2026 liên quan đến công tác bảo đảm an ninh mạng, gồm: **Luật An ninh mạng số 116/2025/QH15** ngày 10/12/2025 và **Thông tư số 48/2026/TT-BCA** ngày 12/5/2026 của Bộ Công an ban hành Quy chuẩn kỹ thuật quốc gia về thiết bị camera giám sát sử dụng giao thức Internet - Các yêu cầu an ninh mạng cơ bản.

2. Rà soát, tăng cường các biện pháp bảo đảm an ninh mạng đối với hoạt động giao dịch chứng khoán trực tuyến

- Rà soát, đánh giá nguy cơ, rủi ro đối với hệ thống giao dịch chứng khoán trực tuyến và quy trình xác thực điện tử; kịp thời khắc phục các điểm yếu, lỗ hổng; tăng cường các biện pháp bảo đảm an toàn đối với hoạt động mở, đóng tài khoản và giao dịch chứng khoán trực tuyến, đặc biệt đối với các quy trình có áp dụng xác thực sinh trắc học.

- Kiểm soát chặt chẽ việc thay đổi thiết bị truy cập, thiết bị xác thực và thông tin tài khoản giao dịch; tăng cường giám sát, kịp thời phát hiện, ngăn chặn các hành vi giả mạo, gian lận hoặc có dấu hiệu tấn công vào hệ thống; thực hiện đầy đủ các quy định của pháp luật về giao dịch điện tử, dữ liệu số, an ninh mạng, bảo vệ dữ liệu cá nhân và các quy định pháp luật có liên quan.

- Chủ động kiểm tra, đánh giá định kỳ mức độ an toàn của hệ thống thông tin; tăng cường áp dụng các giải pháp kỹ thuật nhằm phát hiện sớm, phòng ngừa và ứng phó với các nguy cơ mất an toàn thông tin.

- Trường hợp phát hiện dấu hiệu tấn công mạng, giả mạo sinh trắc học hoặc các hành vi có dấu hiệu vi phạm pháp luật ảnh hưởng đến hoạt động giao dịch chứng khoán trực tuyến, đề nghị Quý Công ty chủ động triển khai các biện pháp xử lý theo quy định; đồng thời phối hợp với cơ quan công an và thông báo kịp thời cho Ủy ban Chứng khoán Nhà nước để phối hợp xử lý theo quy định.

Ủy ban Chứng khoán Nhà nước thông báo để Quý Công ty biết và nghiêm túc triển khai thực hiện.

Nơi nhận:

- Như trên;
- Chủ tịch UBCK (để b/c);
- Cục CNTT-BTC (để b/c);
- Công an Thành phố Hà Nội (để p/h);
- VNX, HNX, HOSE, VSDC (để p/h);
- Ban QLKD, Ban QLQ (để p/h);
- Lưu: VT, CDS (142b).

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH



Hoàng Văn Thu



PHỤ LỤC

MỘT SỐ NGUY CƠ, PHƯƠNG THỨC, THỦ ĐOẠN MỚI CỦA TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO ĐỐI VỚI HOẠT ĐỘNG GIAO DỊCH ĐIỆN TỬ TRÊN THỊ TRƯỜNG CHỨNG KHOÁN

(Kèm theo Công văn số 6486/UBCK-CĐS ngày 14 tháng 7 năm 2026 của Ủy ban Chứng khoán Nhà nước)

Thời gian gần đây, cơ quan công an đã cảnh báo về các phương thức, thủ đoạn mới của tội phạm sử dụng công nghệ cao nhằm lợi dụng các cơ chế xác thực điện tử, đặc biệt là xác thực sinh trắc học, để thực hiện hành vi chiếm đoạt tài sản. Để chủ động phòng ngừa rủi ro, các Công ty lưu ý một số nội dung cơ bản sau:

1. Một số nguy cơ cần lưu ý

- Lợi dụng lỗ hổng hoặc điểm yếu của thiết bị đầu cuối để làm sai lệch kết quả đánh giá mức độ an toàn của thiết bị phục vụ giao dịch điện tử.
- Lợi dụng các sơ hở trong quy trình xác thực điện tử, đặc biệt là xác thực sinh trắc học, để giả mạo danh tính người sử dụng.
- Thay đổi trái phép thiết bị truy cập, thông tin xác thực hoặc tài khoản giao dịch nhằm chiếm quyền sử dụng tài khoản của khách hàng.
- Khai thác các điểm yếu trong quy trình quản trị, vận hành hệ thống hoặc quản lý tài khoản để thực hiện các giao dịch trái phép.

2. Dấu hiệu cần tăng cường giám sát

Các Công ty cần thiết lập cơ chế giám sát, phát hiện sớm đối với các trường hợp như:

- Tài khoản phát sinh yêu cầu thay đổi thiết bị truy cập, thiết bị xác thực hoặc thông tin đăng nhập trong thời gian ngắn.
- Tài khoản đăng nhập từ thiết bị, địa chỉ mạng hoặc vị trí địa lý bất thường so với lịch sử sử dụng.
- Hoạt động xác thực hoặc giao dịch có dấu hiệu bất thường, tần suất cao hoặc không phù hợp với hành vi giao dịch thông thường của khách hàng.
- Thiết bị hoặc môi trường thực hiện giao dịch có dấu hiệu không bảo đảm tính toàn vẹn, độ tin cậy hoặc có nguy cơ bị can thiệp.