

Mất tiền tỷ vì smartphone bị tin tặc chiếm, cách nhận biết và xóa mã độc

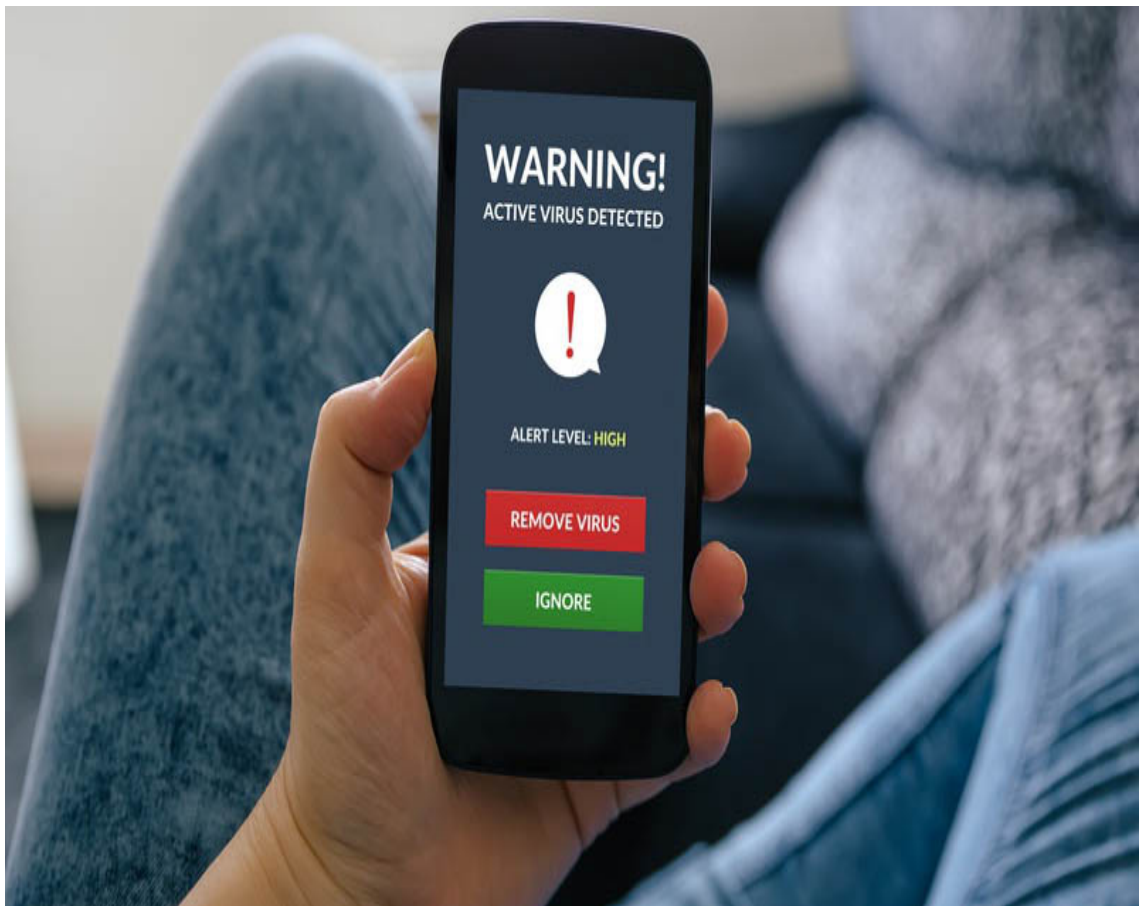
16:22 26/03/2024

Nhiều vụ mất tiền tỷ trong tài khoản ngân hàng, từ chính điện thoại của người dùng khi nhỡ tay bấm vào đường link hay tải ứng dụng. Các chuyên gia công nghệ khuyến cáo, những trường hợp mất tiền như vậy là do smartphone của người dùng đã dính mã độc...



Nhiều v mt tin trong tài khon ngân hàng vì in thoi nhim mã c

Sự việc tài khoản của bà Nguyễn Thị Giang H, Chủ tịch UBND huyện Nhơn Trạch, tỉnh Đồng Nai bị "bốc hơi" 170 tỷ đồng từ ngày 3/3 - 11/3 là mới đây lại khiến nhiều người dùng lo lắng. Không chỉ trường hợp bà H, có rất nhiều người bỗng dưng mất tiền trong tài khoản mà không hề nhận được một thông báo nào.



Trước đó, vào tháng 2, một người đàn ông sống tại quận Hoàn Kiếm, Hà Nội, cũng đã bị mất 3 tỷ đồng trong tài khoản ngân hàng vì cài đặt nhầm mã độc vào smartphone. Những kẻ lừa đảo đã mạo danh mã độc dưới dạng ứng dụng cung cấp dịch vụ công và lừa nạn nhân cài đặt lên smartphone, sau đó kẻ xấu xâm nhập vào ứng dụng chứng khoán của nạn nhân và chiếm đoạt trái phép số tiền 3 tỷ đồng.

Cũng bằng thủ đoạn tương tự, trong tháng 1/2024, thông tin từ Công an TP Hà Nội cung cấp thông tin, có 6 nạn nhân cũng đã bị những kẻ tội phạm công nghệ cao sử dụng chiêu lừa ứng dụng độc hại, mạo danh các ứng dụng dịch vụ công, chiếm đoạt tổng số tài sản lên đến gần 20,6 tỷ đồng, trong đó nạn nhân chịu thiệt hại cao nhất lên đến 15 tỷ đồng.

Theo lãnh đạo Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao (A05), Bộ Công an, hoạt động lừa đảo chiếm đoạt trên không gian mạng không phải là mới nhưng ngày càng tinh vi.

Theo A05, trước đây cơ quan chức năng tập trung phòng chống trên mạng xã hội nhưng gần đây xuất hiện một số ứng dụng lừa đảo. Hiện A05 đang tập trung tuyên truyền cho người dân để nâng cao cảnh giác đối với loại tội phạm này.

Các loại mã độc và ứng dụng gián điệp này cho phép tin tặc xâm nhập trái phép vào ứng dụng ngân hàng cài đặt trên smartphone của người dùng hoặc đọc trộm các tin nhắn chứa mã xác nhận, mã OTP, từ đó đăng nhập vào tài khoản ngân hàng và rút sạch tiền có trong đó.

Những kiểu lừa cài mã độc dưới danh nghĩa ứng dụng

Để xâm nhập trái phép vào điện thoại người dùng và đánh cắp các thông tin tài khoản ngân hàng trên, nhóm tội phạm là lừa nạn nhân cài đặt các loại ứng dụng có chứa mã độc và ứng dụng gián điệp dưới danh nghĩa giả các ứng dụng dịch vụ công, sổ sức khỏe điện tử, sổ Bảo hiểm xã hội...



Thông thường, chúng gọi điện hoặc liên hệ trực tiếp với các nạn nhân mà chúng nhắm đến thông qua Zalo, giả danh là đại diện cơ quan chức năng, yêu cầu người dùng cài đặt các ứng dụng do chúng cung cấp, với lý do đây là những ứng dụng phục vụ cho các dịch vụ công hoặc để khai báo thông tin về nhân khẩu...

Do đây là những ứng dụng chứa mã độc và không được phát hành trực tiếp trên các kho ứng dụng chính thức của Android và iOS, những kẻ lừa đảo sẽ hướng dẫn cho người dùng chi tiết cách cài đặt các ứng dụng, bao gồm cả cấp quyền

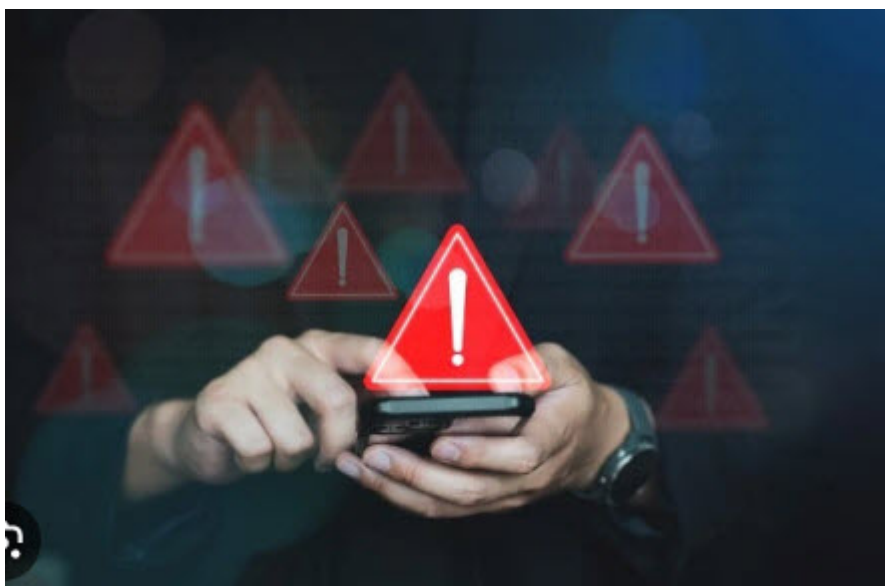
cho phép những ứng dụng này truy cập sâu vào bên trong smartphone để xem trộm và lấy cắp các thông tin nhạy cảm, như đọc trộm tin nhắn, lấy cắp mật khẩu đăng nhập tài khoản, chiếm quyền kiểm soát điện thoại từ xa...

Một số ứng dụng độc hại và gián điệp tinh vi còn yêu cầu người dùng nhập dữ liệu về gương mặt hoặc vân tay để lấy cắp, hoặc chia sẻ những nội dung nhạy cảm và kích thích trí tò mò khiến người xem bấm vào hình ảnh, rồi hướng dẫn quét tiếp hình ảnh mã QR để xem thông tin đầy đủ...

Tuy nhiên, sau khi cài đặt các ứng dụng này, smartphone người dùng sẽ bị kẻ xấu xâm nhập, theo dõi, lấy cắp thông tin cá nhân, và cuối cùng tiền trong tài khoản ngân hàng của nạn nhân cũng không cánh mà bay...

Cách nhận biết điện thoại đã "dính" mã độc

Trước đây, các chuyên gia thường đánh giá nền tảng iOS của Apple thường an toàn hơn Android của Google. Tuy nhiên, hiện tại, nền tảng nào cũng đều có thể bị tấn công nếu người dùng thiếu cẩn thận.



Khi dính mã độc, điện thoại của bạn dù ít hoạt động vẫn hao pin rất nhanh

Dấu hiệu như điện thoại bị chậm, dù không nâng cấp phiên bản mới cũng có thể là dấu hiệu smartphone bị nhiễm độc. Bởi các loại mã độc và ứng dụng gián điệp thường chạy ngầm trên thiết bị sẽ chiếm một khoản không nhỏ tài nguyên hệ thống (CPU, bộ nhớ RAM...).

Một dấu hiệu khác đó là khi pin sụt nhanh dù bạn ít sử dụng điện thoại, chính các hoạt động ngầm của các mã độc khiến pin hao rất nhanh.

Cách kiểm tra để biết ứng dụng nào "ngốn" nhiều pin là vào "Quản lý pin" trên thiết bị, thấy ứng dụng nào khả nghi tiêu hao nhiều pin nhất thì nên gỡ.

Bên cạnh đó, nếu điện thoại hay bị nóng bất thường, trên khay hệ thống xuất hiện những biểu tượng lạ, không rõ của ứng dụng nào, cũng có thể nghi ngờ smartphone đang nhiễm mã độc.

Trong trường hợp smartphone đang có kết nối internet và bạn không sử dụng bất kỳ ứng dụng internet nào (duyệt web, xem video trên Youtube hay sử dụng mạng xã hội...), cũng như không có quá trình nâng cấp nào trên thiết bị, nhưng vẫn có dữ liệu được gửi/nhận trên smartphone, thì rất có thể thiết bị của bạn đã bị dính ứng dụng gián điệp và các ứng dụng này đang gửi/nhận dữ liệu từ smartphone ra bên ngoài mà người dùng không hay biết.

Một dấu hiệu khác nữa, nếu nhận thấy có hiện tượng trình duyệt web tự động mở hoặc chuyển sang các trang web lạ, nhiều khả năng smartphone đã bị nhiễm mã độc.

Khi điện thoại nhiễm mã độc, giải pháp an toàn nhất là khôi phục lại thiết bị về trạng thái nguyên gốc (khôi phục cài đặt của nhà sản xuất) để đưa thiết bị về trạng thái như khi mới xuất xưởng, điều này giúp xóa sạch những ứng dụng (trong đó có ứng dụng độc hại) đã xâm nhập vào hệ thống.

Tuy nhiên, để thực hiện điều này, người dùng cần phải sao lưu toàn bộ dữ liệu trên thiết bị của mình (lưu ý chỉ sao lưu các dữ liệu như hình ảnh, danh bạ, tin nhắn... không sao lưu các ứng dụng).

H. Thủy (Nguồn: <https://www.baogiaothong.vn/>)