6Social Engineering

Trong bối cảnh bảo mật thông tin, kỹ thuật xã hội là quá trình sử dụng

kỹ năng xã hội để thuyết phục mọi người tiết lộ thông tin đăng nhập hoặc các thông tin có giá trị khác

thông tin cho kẻ tấn công. Có một số kỹ thuật kỹ thuật xã hội, mà

thường liên quan đến một thủ phạm đóng giả là một người cao hơn trong tổ chức

thứ bậc cao hơn nạn nhân. Để chuẩn bị cho sự trình bày sai sự thật này, thủ phạm

có thể đã sử dụng các chiến thuật kỹ thuật xã hội chống lại những người khác trong tổ chức để

thu thập thông tin dường như không liên quan, khi được sử dụng cùng nhau, tạo ra thông tin sai

đại diện đáng tin cậy hơn. Chẳng hạn, bất kỳ ai cũng có thể kiểm tra trang web của công ty

trang web, hoặc thậm chí gọi tổng đài chính để lấy tên của CIO; kẻ tấn công có thể

sau đó có được nhiều thông tin hơn bằng cách gọi cho những người khác trong công ty và khẳng định thẩm quyền (sai) của mình bằng cách đề cập đến tên của CIO. Kỹ thuật xã hội

các cuộc tấn công có thể liên quan đến các cá nhân giả làm nhân viên mới hoặc nhân viên hiện tại

yêu cầu hỗ trợ để tránh bị sa thải. Đôi khi những kẻ tấn công đe dọa, dụ dỗ,

hoặc cầu xin để lắc lư mục tiêu.

Có nhiều cuộc tấn công khác liên quan đến kỹ thuật xã hội. một trong số đó là

Phishing

- một nỗ lực để có được thông tin cá nhân hoặc thông tin tài chính từ một cá nhân,

thường bằng cách đặt ra như một thực thể hợp pháp. Một biến thể là lừa đảo trực tuyến, một nhãn mà

áp dụng cho mọi cuộc tấn công lừa đảo có mục tiêu cao. Trong khi các cuộc tấn công lừa đảo bình thường

nhắm mục tiêu càng nhiều người nhận càng tốt, một kẻ lừa đảo giáo sẽ gửi một thông báo xuất hiện

là từ một chủ nhân, một đồng nghiệp, hoặc phóng viên hợp pháp khác, để một nhỏ

nhóm hoặc thậm chí một người cụ thể. Cuộc tấn công này đôi khi được sử dụng để nhắm mục tiêu những

người sử dụng một sản phẩm hoặc trang web nhất định. Các cuộc tấn công lừa đảo sử dụng ba chính

các kỹ thuật, thường kết hợp với nhau: Thao tác URL, Trang web

giả mạo và lừa đảo qua điện thoại.