UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Information Technology Services

Information and Cybersecurity Awareness

Email ithelp@up.ac.za | **www.up.ac.za/itsecurity**

Social Engineering

'Think before you click, like or share'

It doesn't matter if you have locks and bolts on all your doors and windows, guard dogs, alarm systems, floodlights, electrified fences, and armed security personnel; if you open the gate for the person who says he is the pizza delivery guy without first checking to see if he is legitimate, you are completely exposed to whatever risk he represents.

(Source: https://www.webroot.com)

Introduction

Social engineering is the act of tricking or manipulating people to perform specific actions or divulge confidential information. Because of people's inherent curiosity, desire to be kind, and to submit to authority, cybercriminals find this psychological approach easier than bypassing layers of sophisticated technical security controls.

A local example of a successful social engineering attack is the 2020 Experian security breach. Personal information of 24 million people and nearly 800 000 businesses was shared with a fraudster pretending to be a legitimate client.

SEE MORE

▶ WATCH: A real vishing example

READ MORE

The psychology behind social engineering
Poster: Danger signs and what to do

DO MORE

Act like a human firewall, analysing all messages before responding

Typical forms of social engineering attacks are:

- Phishing—an email claiming to be from a source that you trust, e.g. your bank or email service provider, prompting you to enter your login details;
- Vishing (voice phishing)—phishing over the phone;
- Smishing—phishing via SMS;
- Impersonation—pretending to be another person to gain access to a system, information or a physical location.

How to protect yourself

Be on the lookout for these specific techniques that cybercriminals are using with great success:

- CEO fraud—the attackers pretend to be your manager or a figure of authority asking you to perform a task or give them access to sensitive information;
- Spear phishing—a personalised phishing attack using information on the victim collected from public websites and/or social media;
- Messages with infected attachments—the attackers act as if the victim expected or requested the message and attachment, typically a purchase order, invoice or CV;
- An email address from a friend or business connection or a web address that differs from what is expected—look out for misspelling and character replacements, e.g. a small letter l (ℓ) replaced by capital I (ℐ), which looks the same in most fonts.

If unsure, contact the sender to confirm the message using details that you already have and not those provided in the message, or ask advice from a knowledgeable person.

THINK-1 • Graphic sourced and adapted from freepik.com