

Security Awareness Summit & Training

Summit: Dec 3–4
Training: Dec 1–2
Live Online



sans.org/SecAwareSummit

SANS

Security Awareness

Summit & Training

THE HUMAN FIREWALL

A multi-faceted approach to combating Social engineering

Security Awareness Summit & Training

ABOUT THE SPEAKER

JANET MARANGA WESONGA
CISO – UNIVERSITY OF NAIROBI, KENYA

MSc. in Computer Science

CISA

ISO 27001 [ISMS] Lead Implementer

My views and opinions do not represent my employer*

GOAL

Inform: How Social Engineering Works

Persuade: User Education doesn't address SE tactics

Persuade: Best practices to institutionalize

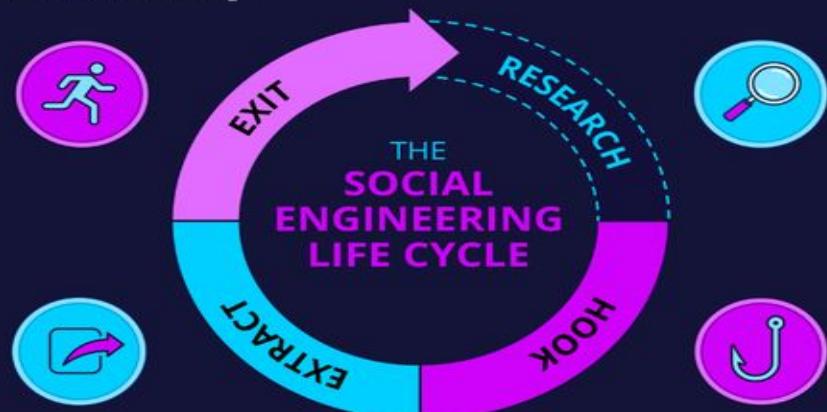
SOCIAL ENGINEERING LIFECYCLE

④ Exit

- allow relationship to end
- provide target with a believable reason for the end of the interaction
- eliminate all evidence of involvement with the target

① Research

- understand the target
- collect background information
- determine the target's weaknesses
- identify the easiest vector of attack



③ Extract

- strengthen relationship with the target
- maintain believability
- leverage control of the relationship with the target
- obtain information from the target

② Hook

- draw the target in
- sell a believable story or promise
- build a relationship with the target
- establish control of the relationship with the target

HUMAN VULNERABILITIES

How Social Engineering attacks work

A photograph of three monkeys on a wooden deck. One monkey is in the foreground, sitting and grooming another monkey's back. A third monkey is sitting to the right, looking towards the camera. In the background, there are more monkeys and some fallen leaves.

RECIPROCITY



The Law of Familiarity



People feel comfortable with
who and what they know

A vintage hand pump stands prominently in the foreground on a dry, cracked earth surface. The pump is made of metal and has a curved handle on top. The background shows a vast, flat, and dry landscape stretching to a distant horizon under a hazy, light-colored sky.

SCARCITY



USER EDUCATION

Doesn't change Human Nature

USER EDUCATION

- ❑ Cannot cover every case
- ❑ Does not “Solve” Reciprocity, Trust, Familiarity, Scarcity and Authority
- ❑ Fades after about 6 months
- ❑ Treats each situation with context



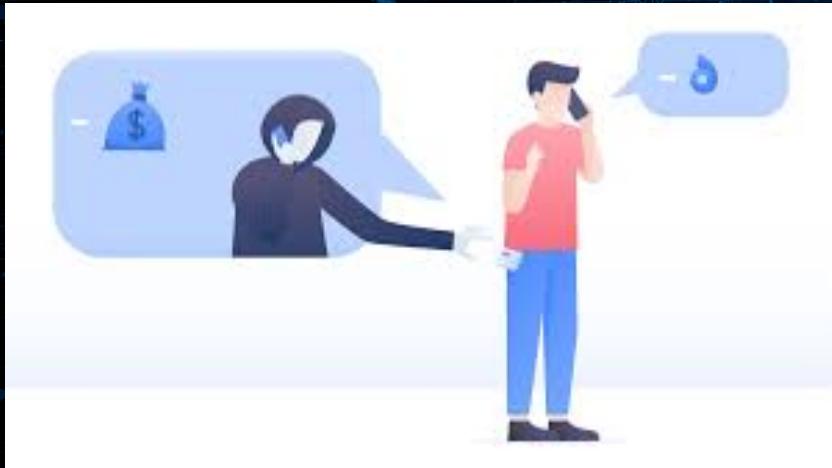
TYPICAL TYPES OF ATTACKS

Phishing



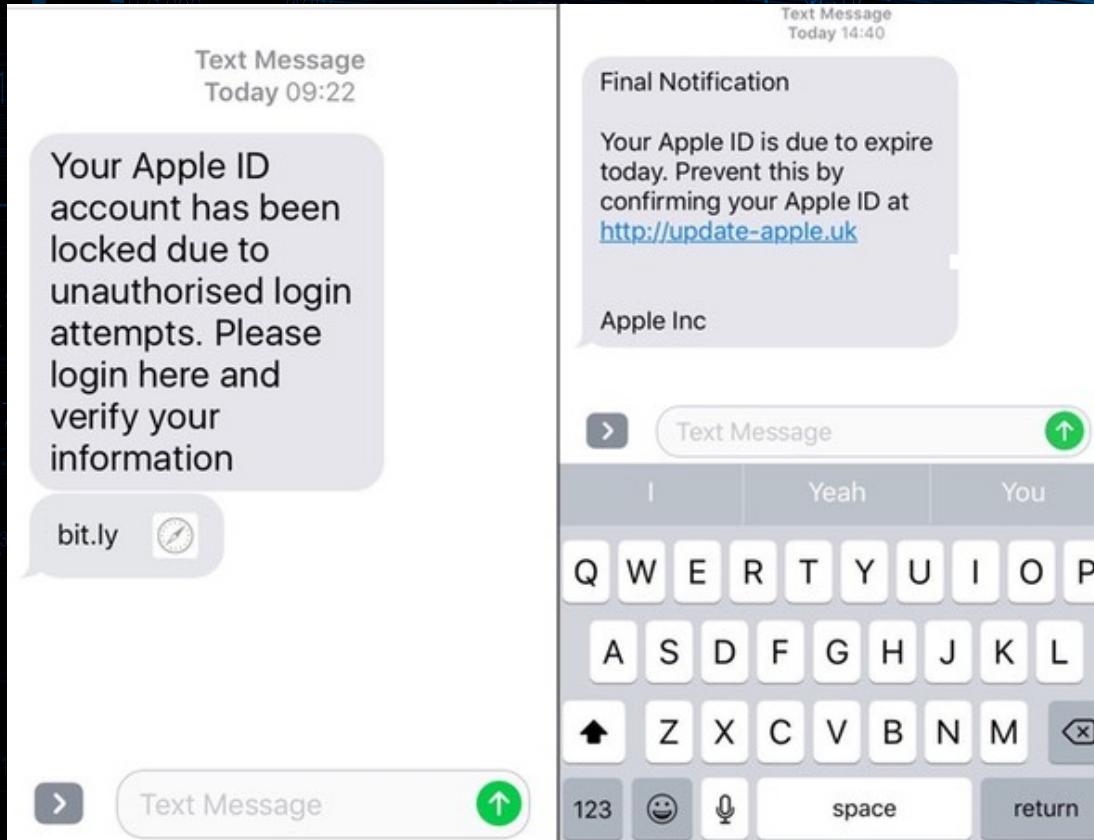
TYPICAL TYPES OF ATTACKS

Vishing



TYPICAL TYPES OF ATTACKS

Smishing



TYPICAL TYPES OF ATTACKS

Passwords



TYPICAL TYPES OF ATTACKS

Pretexting



TYPICAL TYPES OF ATTACKS

Contact Spamming and Email Hacking



TYPICAL TYPES OF ATTACKS

Quid Pro Quo



MITIGATION: Level 1: Research

How can we reduce falling prey to social engineering

DIGITAL FOOTPRINT

Limit Oversharing



MITIGATION: Level 2: Hook

How can we reduce falling prey to social engineering

ALERTNESS



BE SKEPTICAL



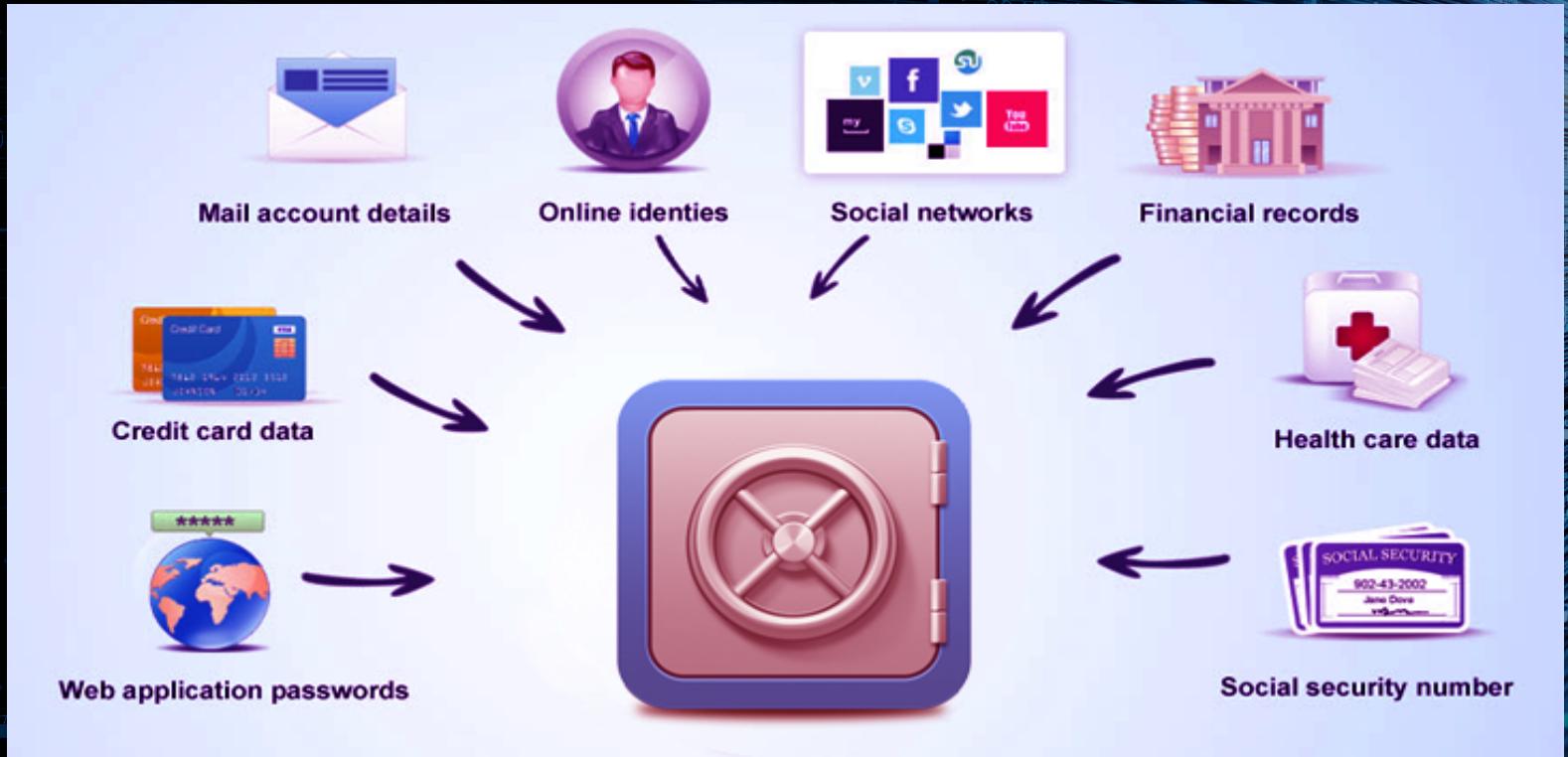
TRUST BUT VERIFY



MITIGATION: Level 3: Extract

How can we reduce falling prey to social engineering

PASSWORDS



DUE DILIGENCE



BASIC SECURITY HYGIENE



MITIGATION: Level 4: Exit

How can we reduce falling prey to social engineering

CALL THEM BACK



MITIGATION: Corporate Level

How can we reduce falling prey to social engineering

EMAILS

Editor

HTML RTF PLAIN TEXT

Save Convert Source Preview Guidelines

Actions Template Library View

Font Paragraph Insert

Header

Header LEFT CONVERSATION RIGHT SIGNATURE/DISCLAIMER

Original message

Attention! This email originates from outside of the organization. Do not open attachments or click links unless you are sure this email comes from a known sender and you know the content is safe.

Hi Robert,

This is what your original message will look like together with the signatures added by CodeTwo Exchange Rules Pro. You can add signatures, disclaimers and banners right below the original message, at the very bottom of the correspondence, and as headers or side-banners. Clicking the Placeholder button will let you choose Active Directory fields that will be turned into users' personal information when the message goes through the server.

SPAM FILTERS

Settings

Email options

- General settings
- Autoresponder
- Sort rules
- Spam options**
- Black/White list

My Account

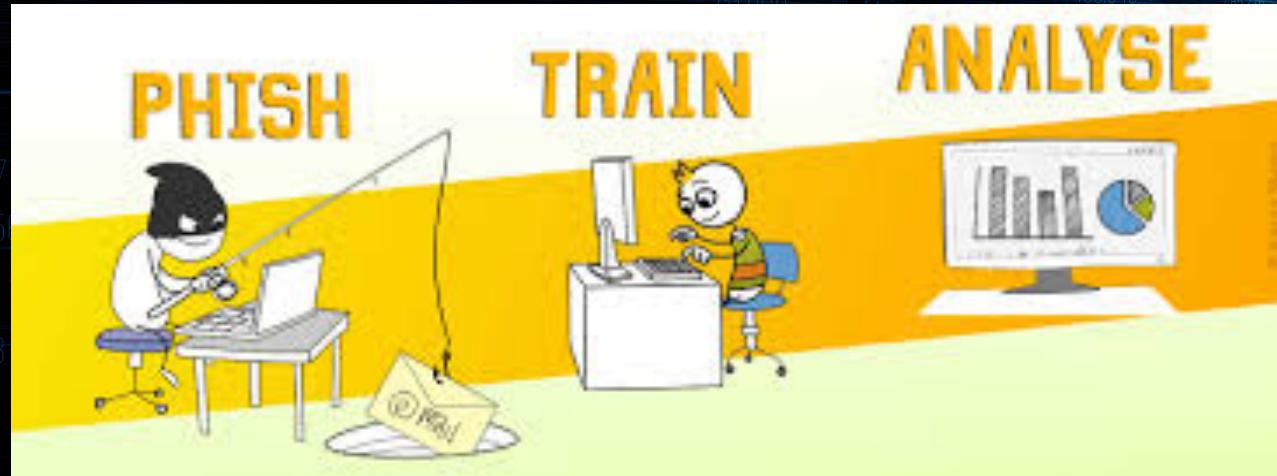
Save settings Cancel

Email: Spam options

Filter level:

- Do not use spam filter** - no emails
- Low** - only most common spams
- Middle** - majority of spams will be
- High** - almost all spams will be

PHISHING SIMULATIONS



PRIVILEGED ACCESS & MFA



CARRY OUT REGULAR CYBERSECURITY POSTURE ASSESSMENTS OF YOUR ENVIRONMENT



CONCLUSION

- Measures covered will help you to mitigate attempts to trick and cajole you or your staff into revealing data
- None of them stands alone
 - Protecting against the sophisticated tactics of cybercriminals to prevent social engineering attacks is a process.
- When the human element of behavior manipulation is added via social engineering this process can have many moving parts
- Human-centric security as well as technological approaches such as 2FA
- A multi-faceted socio-technological approach against social engineering has to be institutionalized to prevent successful SE attacks.

THANK YOU!