Security Awareness

Summit & Training

SANS

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

sans.org/SecAwareSummit

Security Awareness
Summit & Training

THE HUMAN FIREWALL

A multi-faceted approach to combating Social engineering

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*

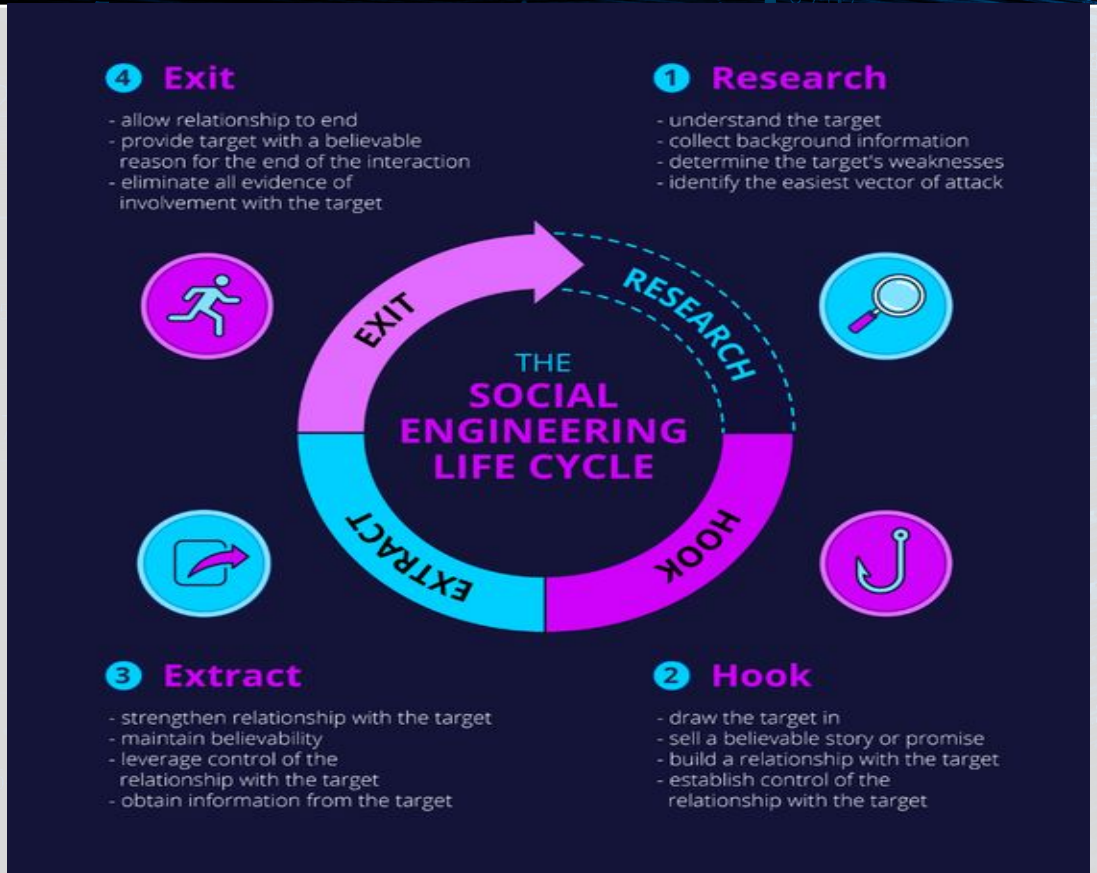
GOAL

Inform: How Social Engineering Works

Persuade: User Education doesn’t address SE tactics

Persuade: Best practices to institutionalize

SOCIAL ENGINEERING LIFECYCLE



HUMAN VULNERABILITIES

How Social Engineering attacks work


RECIPROCITY

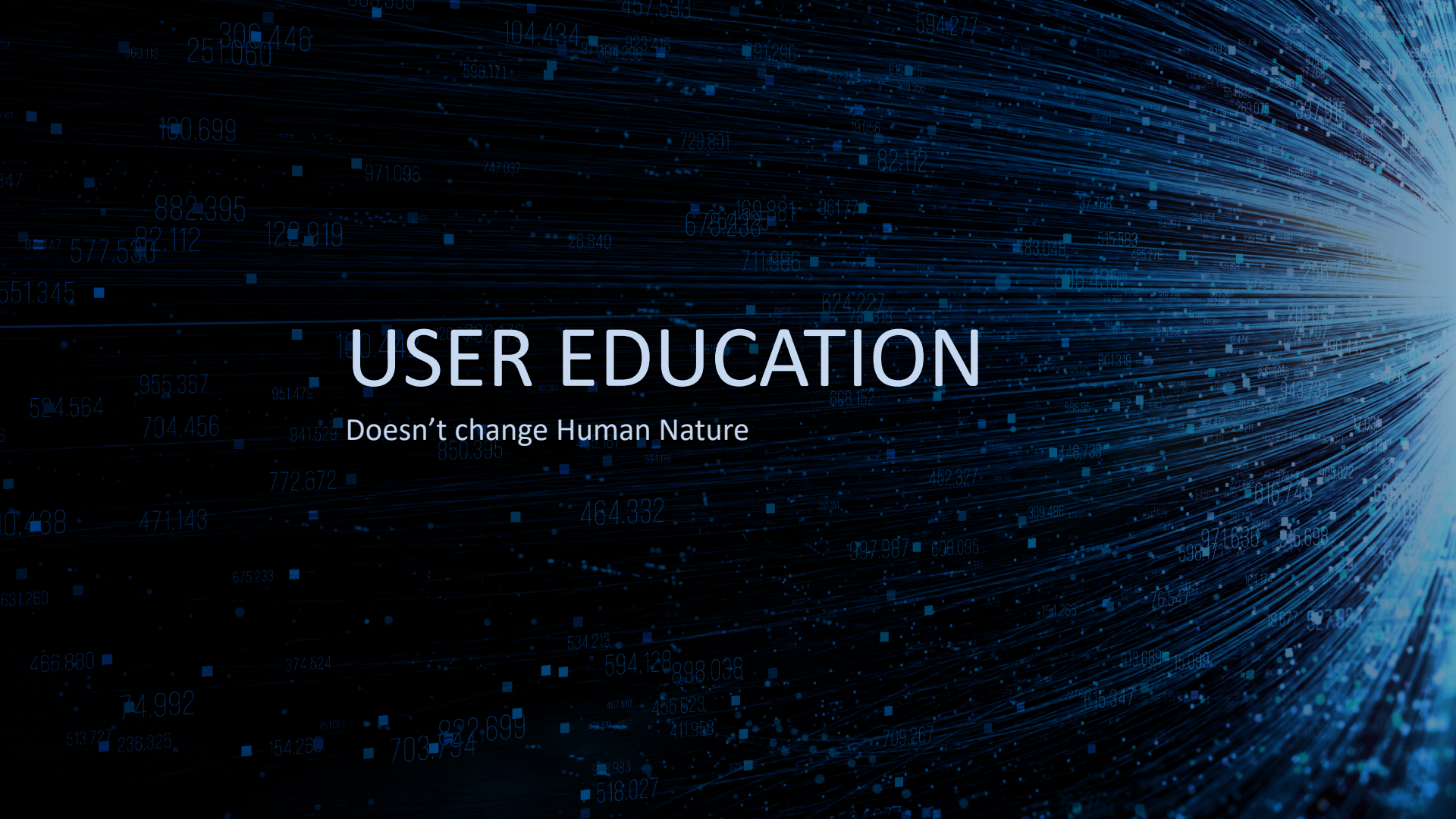

LOW
AVERAGE
HIGH
MAXIMUM
COMMITMENT
Level

The Law of Familiarity

People feel comfortable with who and what they know


SCARCITY


INTELLIGENCE
MISSION
COMPUTER
BUSINESS
PROJECT
POWERFUL
AUTHORITY
FOLLOWERS
SUCCESS
TEAM


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

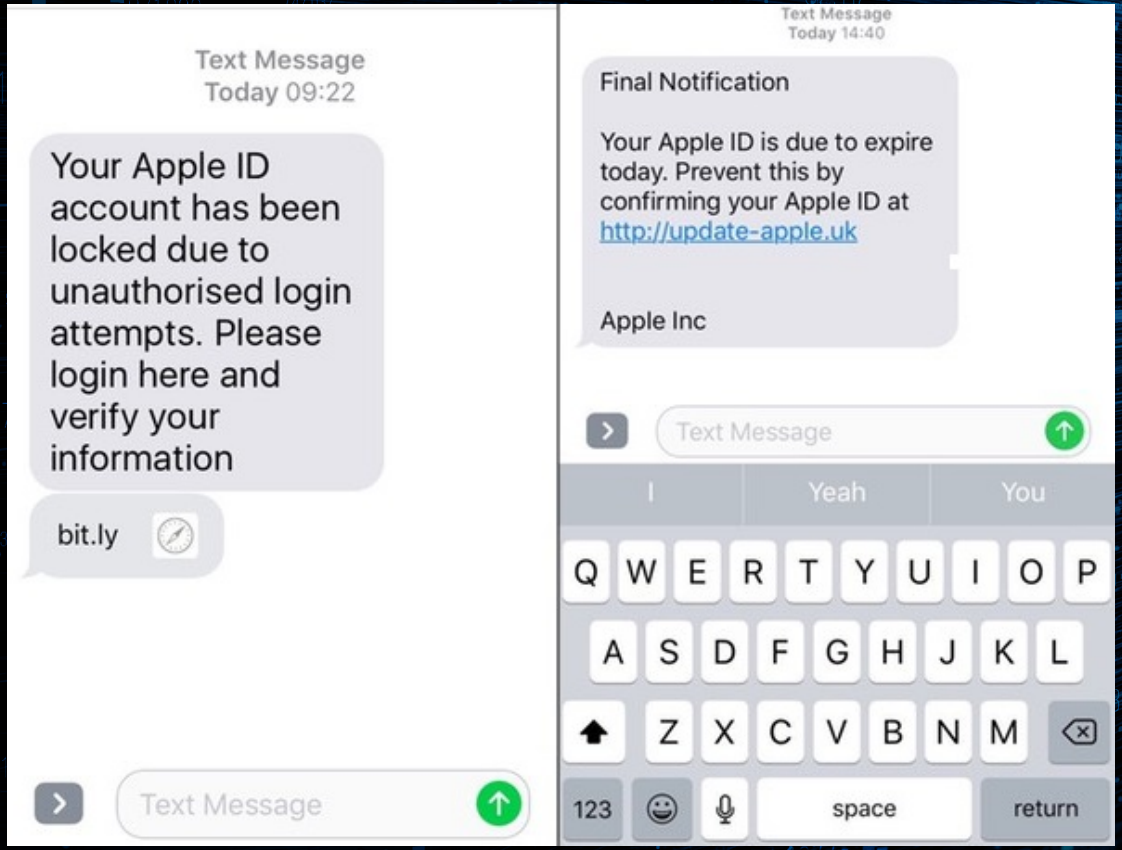
Phishing

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

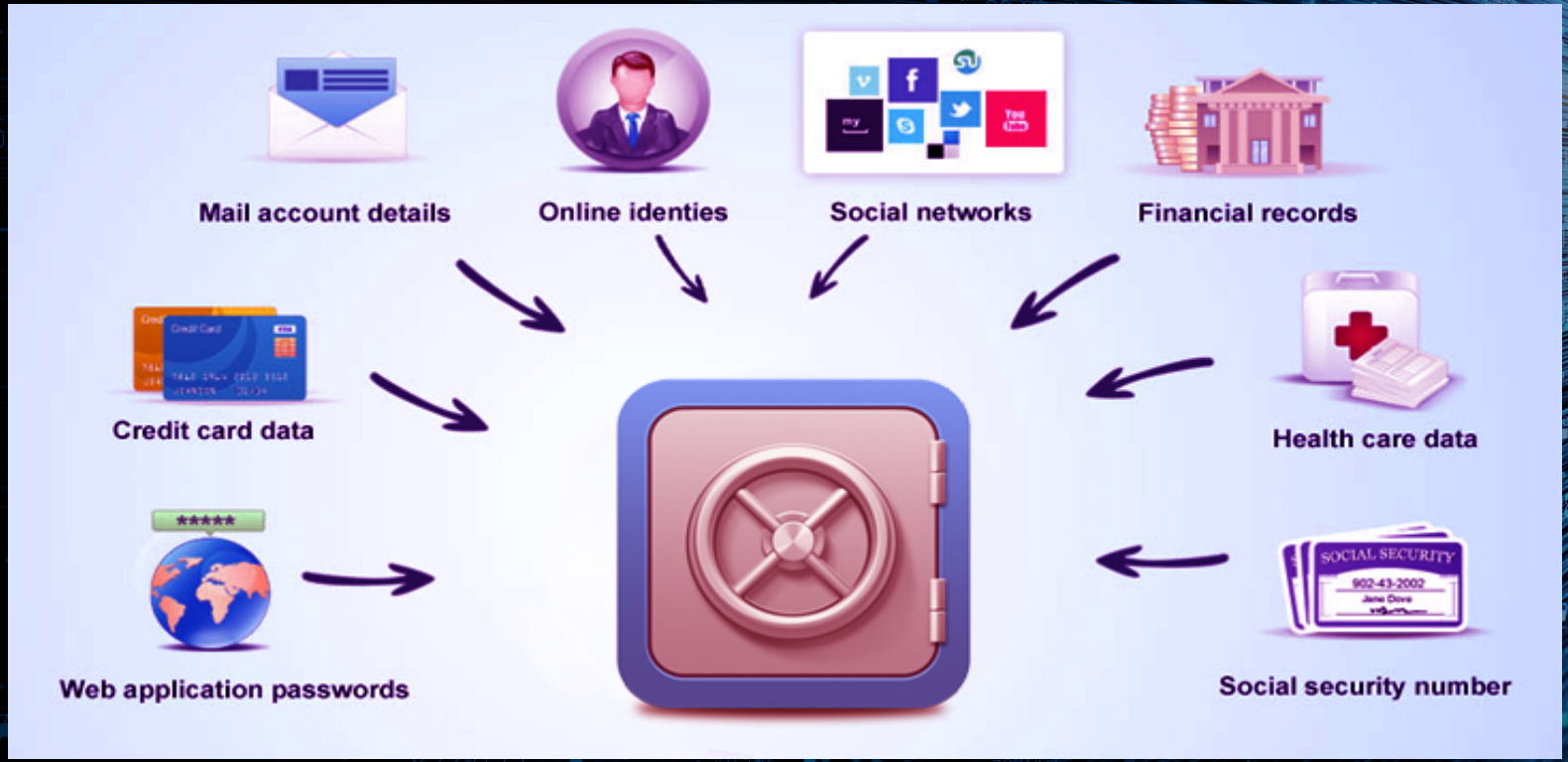
BE SKEPTICAL

TRUST BUT VERIFY

MITIGATION: Level 3: Extract

How can we reduce falling prey to social engineering

PASSWORDS


Mail account details
Online identies
Social networks
Financial records
Credit card data
Health care data
Web application passwords
Social security number
SOCIAL SECURITY
902-43-2002

DUE DILIGENCE

BASIC SECURITY HYGIENE

MITIGATION: Level 4: Exit

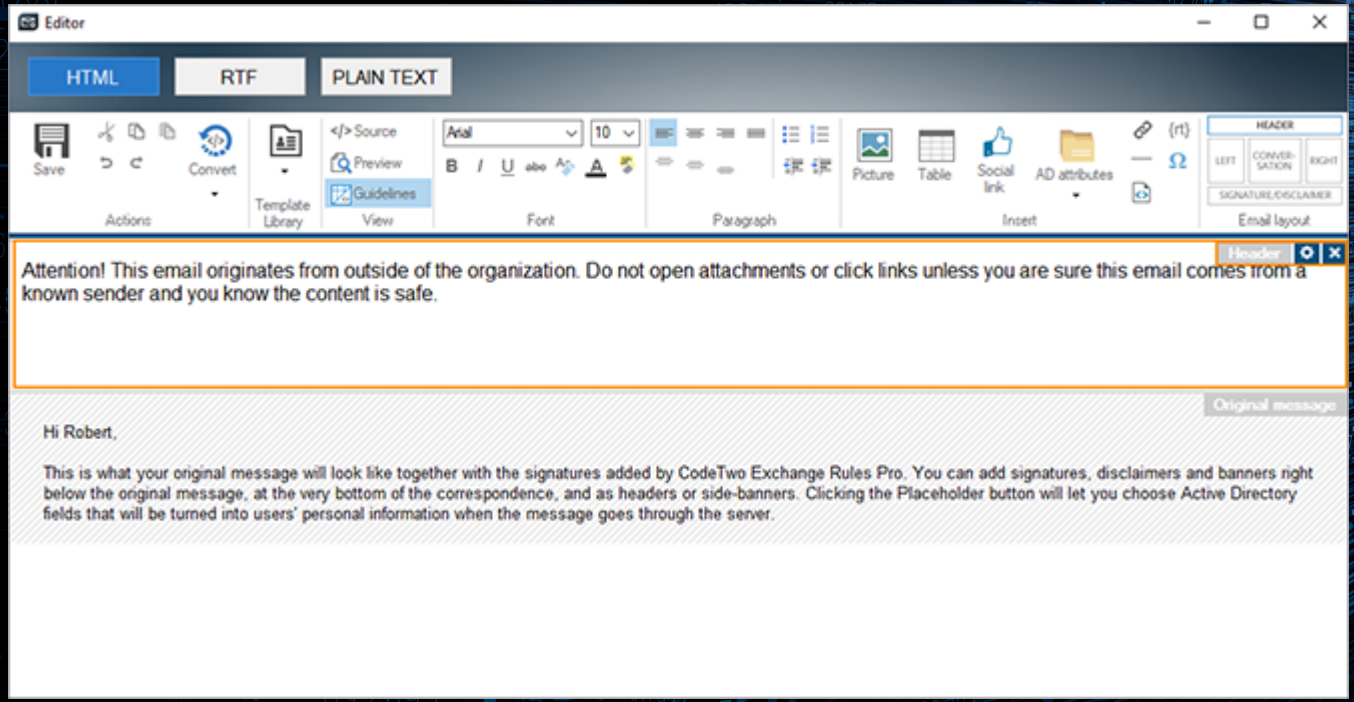
How can we reduce falling prey to social engineering

CALL THEM BACK

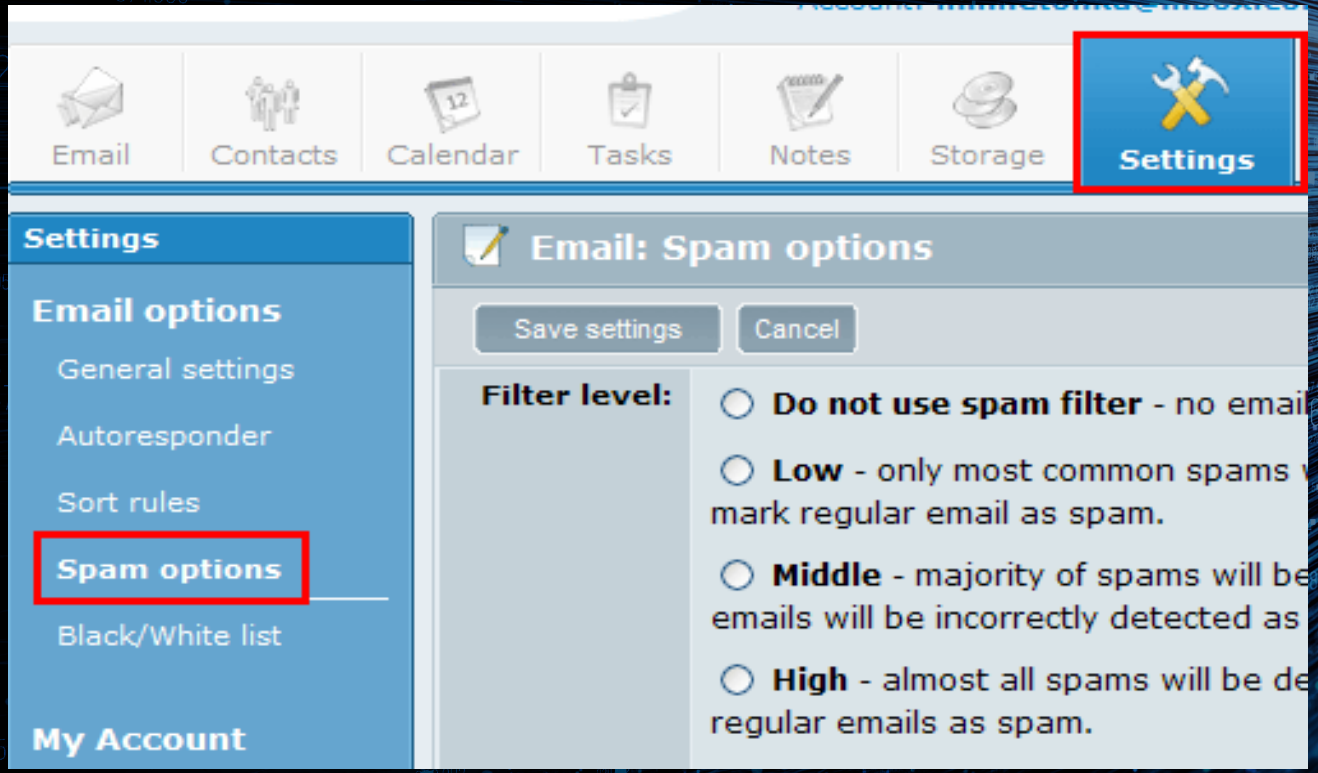
MITIGATION: Corporate Level

How can we reduce falling prey to social engineering

EMAILS


Editor
HTML
RTF
PLAIN TEXT
Save
Convert
Actions
Template Library
Source
Preview
Guidelines
View
Arial
10
Font
Paragraph
Picture
Table
Social link
AD attributes
Insert
HEADER
LEFT
CONVERSATION
RIGHT
SIGNATURE/DISCLAIMER
Email layout
Header
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.
Original message
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



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!