Loss Prevention
QUICK REVIEW
DATA SECURITY

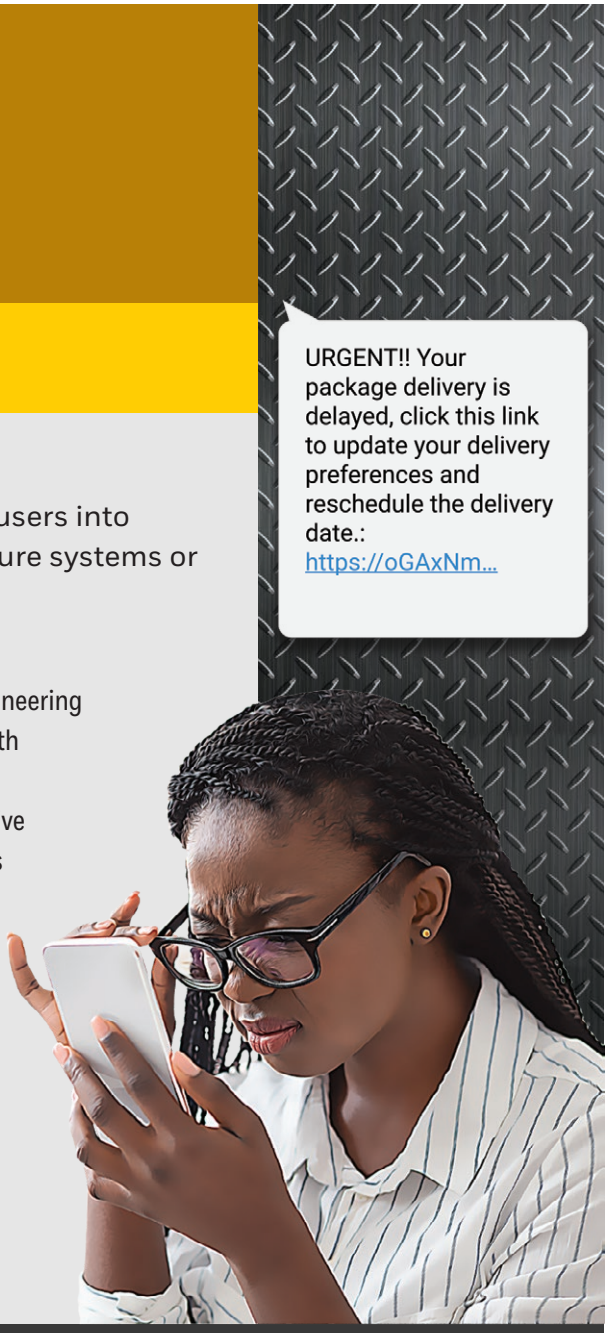
SOCIAL ENGINEERING

WHAT IS SOCIAL ENGINEERING?

Social engineering and phishing attacks attempt to trick users into revealing private information or passwords, access to secure systems or areas.

RECOGNIZING ALL TYPES OF SOCIAL ENGINEERING

- **Requests require fast response or crucial time window:** Social engineering attacks rely upon a person not asking for confirmation or checking with others prior to acting.
- **Threats:** This goes along with rushed requests. There are often negative consequences implied if the request is not completed quickly. Threats of fines, denied access, missed opportunities for easy money or employment termination are common.
- **Unsolicited messages:** Social engineering attacks are not typically in response to a request or other previous communication. Receiving an unsolicited communication should raise suspicions.
- **Requests for sensitive information:** Most attacks ask for passwords, login information, Social Security numbers, bank account numbers, credit card information or other data that is typically kept private or confidential. Requests for this information from any source should be treated with suspicion.



PREVENTION

If a message has one or more of the elements above, you should:

- Contact IT and follow thier directions.
- Forward any requests for private information to the responsible authority for your organization.
- Do not open the message, click on any links or items or follow instructions in the message, such as sending confidential information or passwords.

NOTES:

Click Wisely