THE BEST TECH CAN'T STOP IT!

# The Fundamentals of Social Engineering

**Avery Moore**
Chief Information Security Officer
Jazz Solutions, Inc.
https://www.jazzsolutions.com
https://www.linkedin.com/company/jazzsolutions/

JSL
Engineered to Execute™

**DOL Cybersecurity Awareness Day 2024**

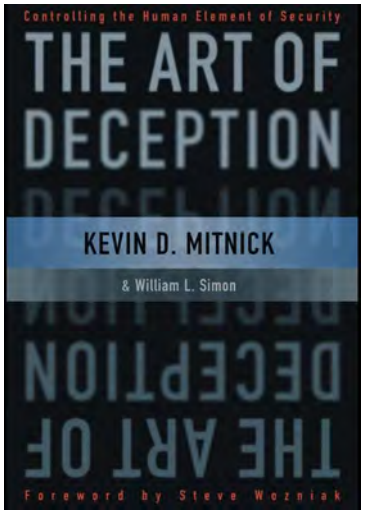
JSL
Engineered to Execute™

v 2.0

# Kevin Mitnick

RIP


- Was a master at using both technical and **non-technical** means to conduct his illegal activities.
- Served prison time due to wire fraud and several other crimes.
- Later became a security consultant.
- The first book he wrote (after getting out of prison) was about **social engineering** (not “hacking”).



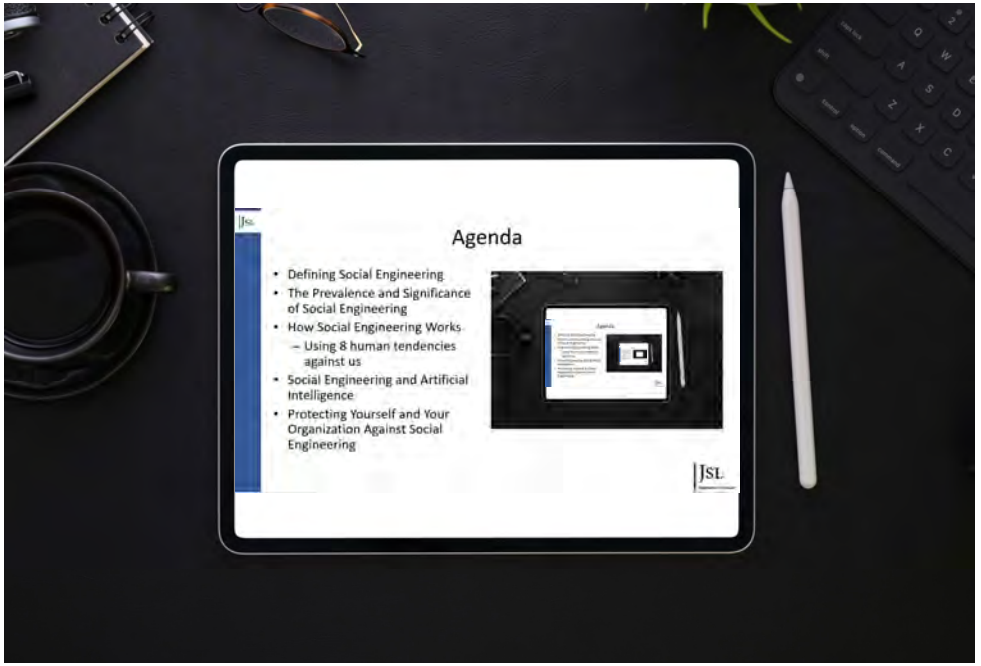
# The Human Factor

*Security is too often merely an illusion, an illusion sometimes made even worse when gullibility, naïveté, or ignorance come into play. The world's most respected scientist of the twentieth century, Albert Einstein, is quoted as saying, "Only two things are infinite, the universe and human stupidity, and I'm not sure about the former." In the end, social engineering attacks can succeed when people are* ***stupid****, or more commonly, simply* ***ignorant*** *about good security practices.*

from *The Art of Deception* by Kevin Mitnick and William Simon, 2002

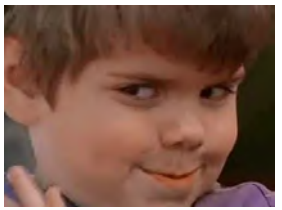
# Agenda

- Defining Social Engineering
- The Prevalence and Significance of Social Engineering
- How Social Engineering Works
  - Using 8 human tendencies against us
- Social Engineering and Artificial Intelligence
- Protecting Yourself and Your Organization Against Social Engineering




Engineered to Execute™

# Defining Social Engineering

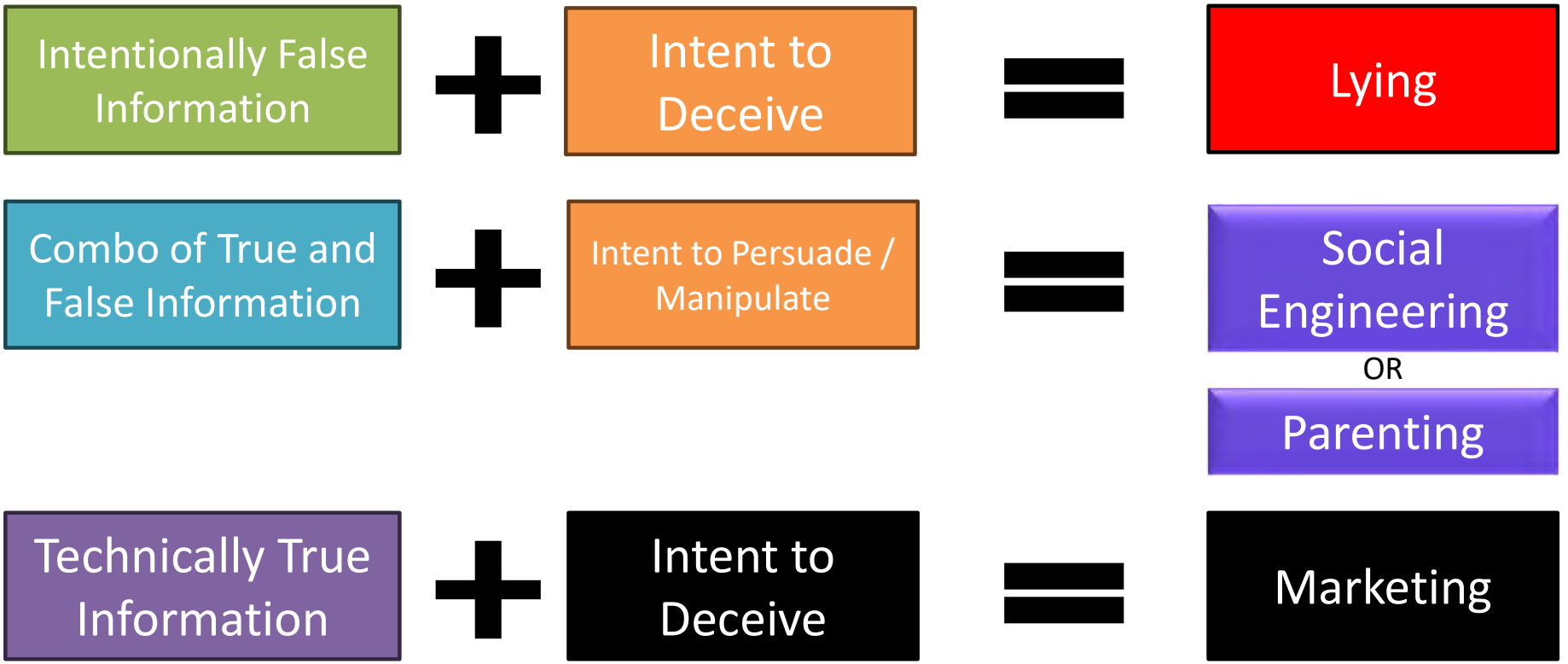


- "Social engineering is any act that **influences** a person to take an action that may or may not be in his or her best interests." Christopher Hadnagy in *Social Engineering: The Science of Human Hacking, Second Edition*, 2018

- "Social Engineering uses **influence** and **persuasion** to **deceive** people by convincing them that the social engineer is someone he is not, or by **manipulation**. As a result, the social engineer is able to take advantage of people to **obtain information** with or without the use of technology." from *The Art of Deception* by Kevin Mitnick and William Simon, 2002

JSL
Engineered to Execute™

# Deception and Untruths



# Patterns: What the Stats Say

Social Engineering

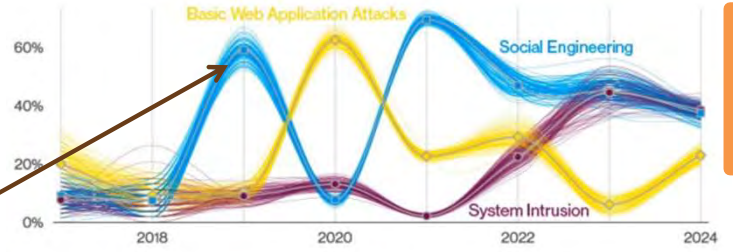



**Figure 76.** Top patterns over time in APAC breaches

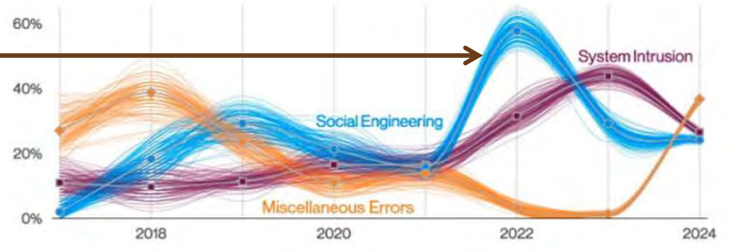



**Figure 77.** Top patterns over time in EMEA breaches

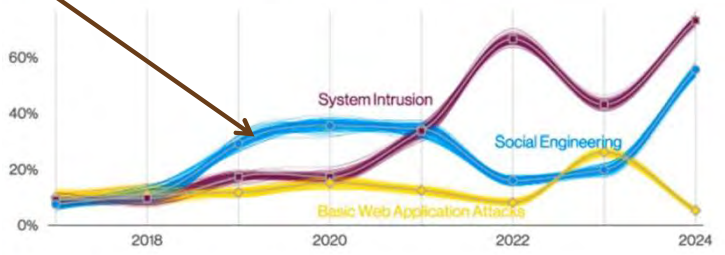



**Figure 78.** Top patterns over time in NA breaches

According to the 2024 DBIR, **Phishing** and **Pretexting** via email continue to be the leading cause of incidents…accounting for 73% of breaches.

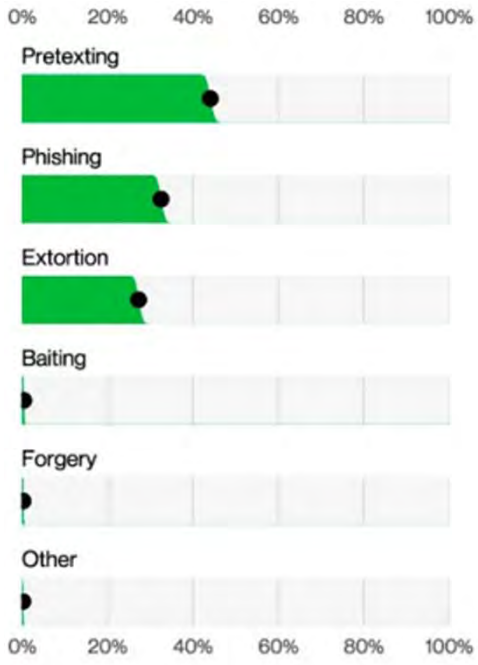



**Figure 34.** Top Action varieties in Social Engineering incidents (n=3,647)

Source: Verizon 2024 Data Breach Investigations Report (verizon.com/dbir/)

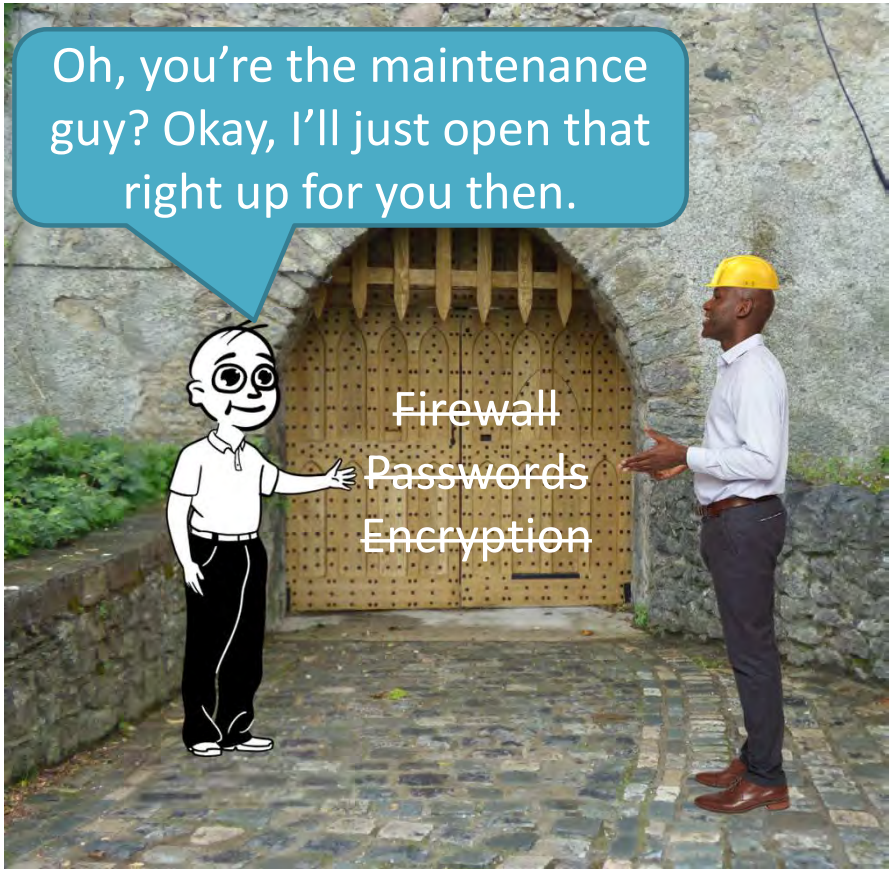
# Social Engineering Goes Around Controls

Social engineering can use a combination of non-technical and technical means as a way of "going around" the typical technical controls that would normally stop or severely slow down an attacker.

Controls such as:

- Firewalls
- Gates / Locked Doors
- Passwords / Authentication
- Encryption

A bad guy probably doesn't even need to "hack their way into" the system. He just walks in the front door and asks for the password.



# How Social Engineering Works

The Breakdown

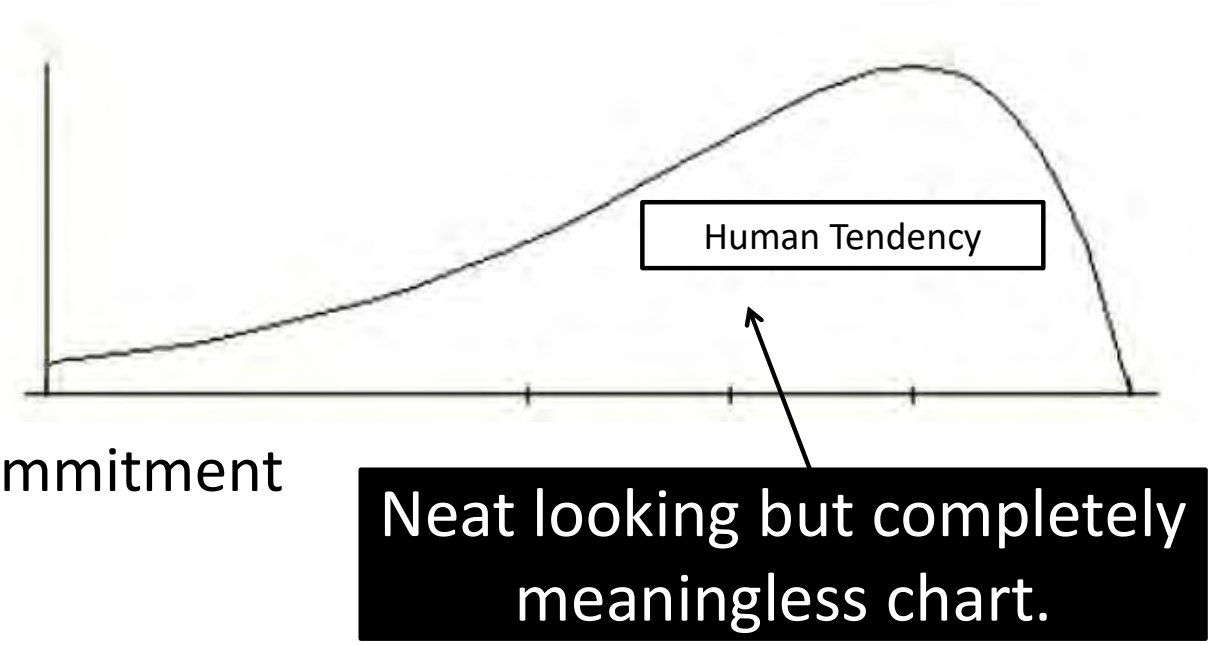

**DOL Cybersecurity Awareness Day 2024**

JSL
Engineered to Execute™

# Social Engineering Exploits Human Tendencies

**Social Engineering exploits the typical human response to these eight concepts:**

1. Reciprocity
2. Obligation
3. Concession
4. Scarcity
5. Authority
6. Consistency and Commitment
7. Liking
8. Social Proof




Concepts borrowed from:

- Christopher Hadnagy in *Social Engineering: The Science of Human Hacking, Second Edition*, 2018
- Robert B. Cialdini in *Influence: The Psychology of Persuasion, Revised Edition, 2018*



JSL Engineered to Execute™

# 1. Reciprocity

The tendency to feel like you should do something in return for someone because they gave something to you.

Here is an example from an actual phishing email I received:

> This is to bring to your notice that, I have paid the courier charges and the delivery of your ATM CARD.I paid it because the ATM CARD worth USD $5.5M has less than Four weeks and four days to expire and when it expires the money will go into Government reserve. With that I decided to help you pay the money so that the ATM CARD will not expire, because I know that when you get your ATM CARD definitely you must compensate me.

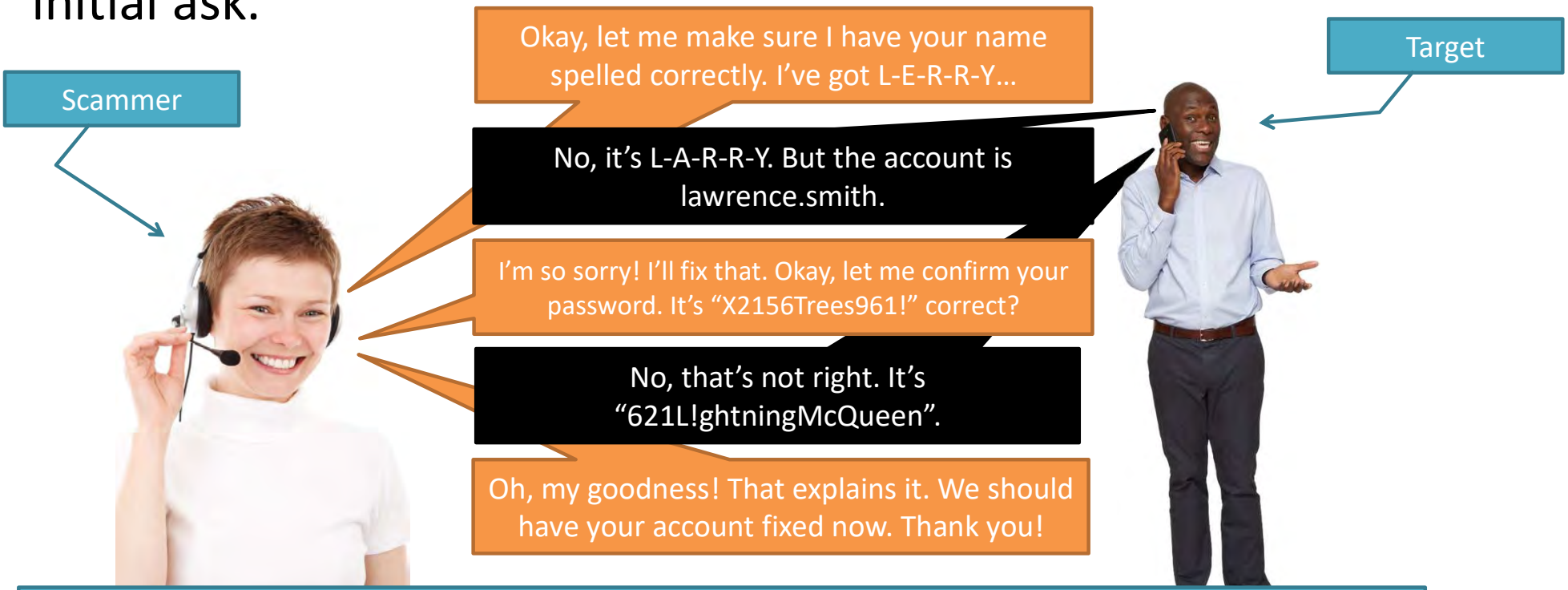
This scammer already “paid the courier charges”. Perhaps I could **reciprocate** by getting the ATM card and paying them back.

# 2. Obligation

This is similar to reciprocity, but it is based on social norms or expected behaviors rather than indebtedness.

# 3. Concession

Uses our tendency to grant a request that is less than the initial ask.




The target, after giving minor information "**concedes**" the major information (password) without even thinking. Phone scammers do this all the time.

"Concede." *Merriam-Webster.com Dictionary*, Merriam-Webster, https://www.merriam-webster.com/dictionary/concede. Accessed 7 Mar. 2022.

JSL
Engineered to Execute™

# 4. Scarcity

The tendency to act on something quickly or without thought or pay a higher price for an item because there is a perception that the supply is limited.

The CEO is on vacation for a couple of weeks. He sent me to fix his laptop while he's gone. I'm super busy and can't get back here for at least **three weeks**.

I don't have you on my list but since you're booked solid, I need to let you do this. I don't want the CEO to be mad. He did mention his computer was slow.

The scarcity in this case is the **availability** of the tech to complete the work.

## Unemployment Benefit Scams

Scammers send phishing emails and SMS messages with links to fake unemployment benefit application websites designed to harvest personally identifiable information (PII) from victims who think they are applying for limited (i.e., scarce) unemployment benefits. Scammers urge would be victims to act quickly to make their claims to discourage rational thought and verification of their legitimacy.

JSL
Engineered to Execute™

# 5. Authority

## The tendency to defer to perceived authority.

Authority and Urgency!

**From:** Kristen Larson <**redacted**@gmail.com>
**Sent on:** Tuesday, October 1, 2024 4:00:07 PM
**To:** **redacted**@jazzsol.com
**Subject**:

Hello,I need you to run an errand for me urgently ,kindly get back to me with your cell for more details.

Kristen Larson
Chief Executive Officer
Jazz Solutions Inc

Possibly the two most powerful props in social engineering:

JSL
Engineered to Execute™

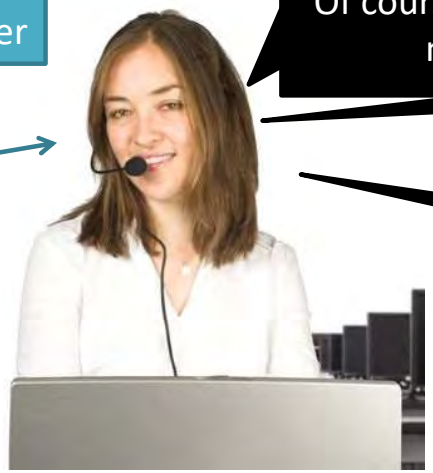
# 6. Consistency and Commitment

We want to appear consistent in the way we respond. Consistency is a sign of confidence and strength. This is also known as the “foot in the door” approach.

This is the security department. We’re reminding employees about our security standards. … Do you agree with those security policies and standards?

Of course, I do!! I care about security and this company.

Scammer



Of course, you do! Now that you understand our password policy, we need to verify that your password meets that standard.

Of course! It’s “L@mbaM0nkeys378~”. That’s pretty strong, right?

Oh, yes, it certainly is. It looks like you’ve met our security requirements. Have a great day!

This concept is constantly used in politics…and sales.

# 7. Liking

As with many things in life, we tend to comply with someone if they are likable and are like us. Social engineers play that card often.

- The scammer will find common ground with the target(s) by searching publicly available sources of information (e.g., social media, etc.) or finding some other source of **common ground**. The best ones can do it on the fly.

Hi, I just noticed your Arizona State University bumper sticker. I'm an ASU alum myself. I'm Jim. I just started here with HR.

You catch more flies [**victims**] with honey than you do with vinegar.

# 8. Social Proof

We respond positively if we think others have responded positively.

We're trying to find the root cause of a problem in the phone lines.

I checked out the lines at the businesses next door and there wasn't a problem there.

I figured since I'm here, I might as well run the test on your line as well.

**Door-to-Door salespeople use this tactic.**

"I have signed up many of your neighbors. See here, Bob, your next-door neighbor, signed up."

JSL
Engineered to Execute™

# Caveats

- The eight tendencies and related examples are **not the only way** to categorize these attacks. You probably have better examples. Good!!
- Social engineering attacks can be perpetrated through **any** medium that allows personal interaction:
  - Telephone
  - Voice mail (i.e., vishing)
  - Email (i.e., phishing)
  - Text messages (i.e., smishing)
  - In-person
  - Video call
  - Walkie-talkie
  - Morse code (that might be a bit of a stretch)

- Good social engineers are **sneaky**.
  - They can use several of your tendencies without you actually knowing it.
  - You must be on your guard.
- Social engineering tactics are typically **not done in isolation**.
  - They are used as gateways to other attacks such as insider fraud.

# BuT wHaT aBoUt AI???

**Implications of Artificial Intelligence (AI) on Social Engineering**

**Attacker Can Use AI to:**

- Craft more convincing phishing emails with proper grammar and made to look/feel like a specific person.
- Impersonate a person's voice and/or likeness (deepfakes).
- Coordinate and automate reconnaissance and attack activities.
- Enhance detection evasion.

**Organizations Can Use AI to:**

- Detect, analyze, respond to social engineering attacks.
- Detect, analyze, respond to deepfakes.
- Compliment and enhance awareness and training efforts.

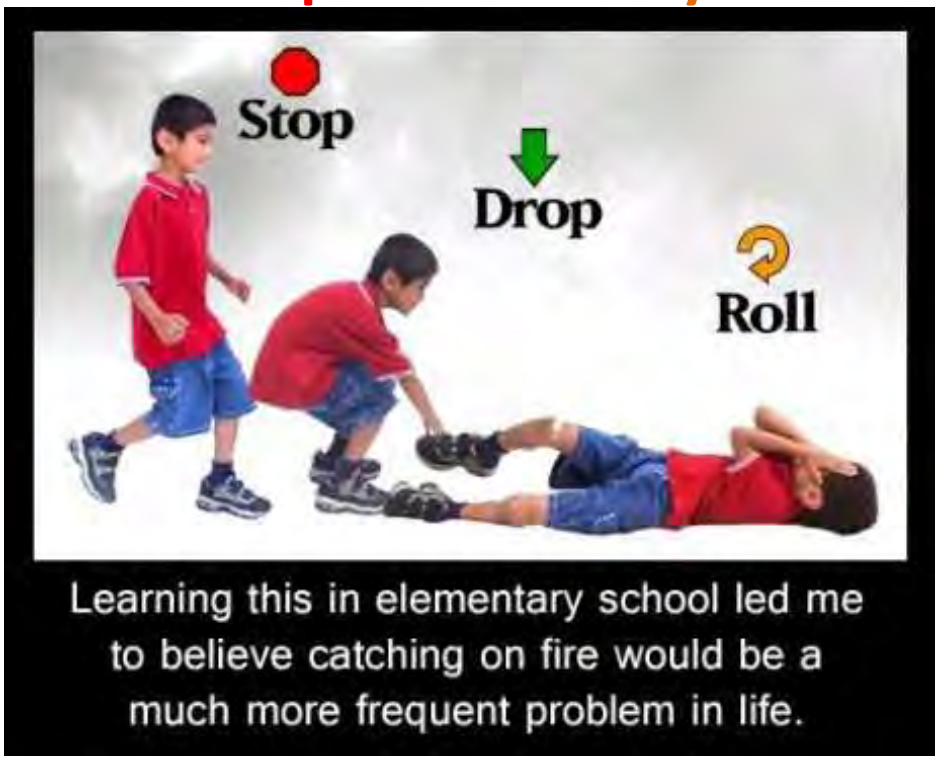
As you know, the implications of AI in EVERYTHING are constantly and rapidly evolving.

JSL
Engineered to Execute™

# Protecting Yourself and Your Organization Against Social Engineering

- Know your own tendencies.
- Understand your exposure. Think like an attacker.
- Don't think you're immune from these attacks.
- **Stop. Think. Verify.**
- Managers and leaders, never punish or ridicule people for verifying.
- Know your organization's policies and standards.
- Know your "always" and "nevers" and stick to them.
- Use your "designated bad guys".
- Report all suspicious activities.

**Stop. Think. Verify.**




JSL
Engineered to Execute™

JSL
Engineered to Execute™

# Record of Success

**100%**
**POSITIVE**
Contractor Performance Assessment Reports on all contracts

**100%**
Recompetes Won

**250 MILLION**
Citizen Interactions for Customers in Federal Government

**20+**
States with JSL Staff

**98%**
AVERAGE
Consistent Employee Retention Rate

**83%**
Staff with IT & PM Certifications

**30+** Contracts

**20+** Prime

"JSL is always the most reliable partner."

– Federal Customer Project Lead

# Thank you!

**Avery Moore**

avery.moore@jazzsol.com


## Jazz Solutions, Inc.

https://www.jazzsolutions.com

https://www.linkedin.com/company/jazzsolutions/

Visit our booth to request a copy of this slide deck.

JSL

Engineered to Execute™