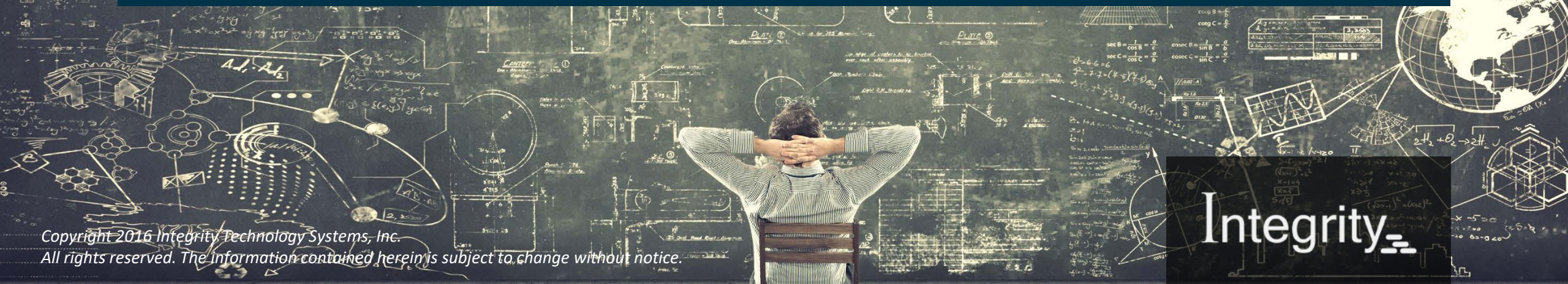
WHAT IS

SOCIAL ENGINEERING?



Integrity

Social Engineering

The hacking of humans

Using knowledge of human behavior to elicit a defined response.

Integrity

Sociology and Psychology

- Study of human behavior, interaction and societal norms.
- Actions can be predicted quite accurately.
- Actions can also be influenced quite easily.

Simple Human Behavior

- Two Types of Responses
  - Natural
  - Learned

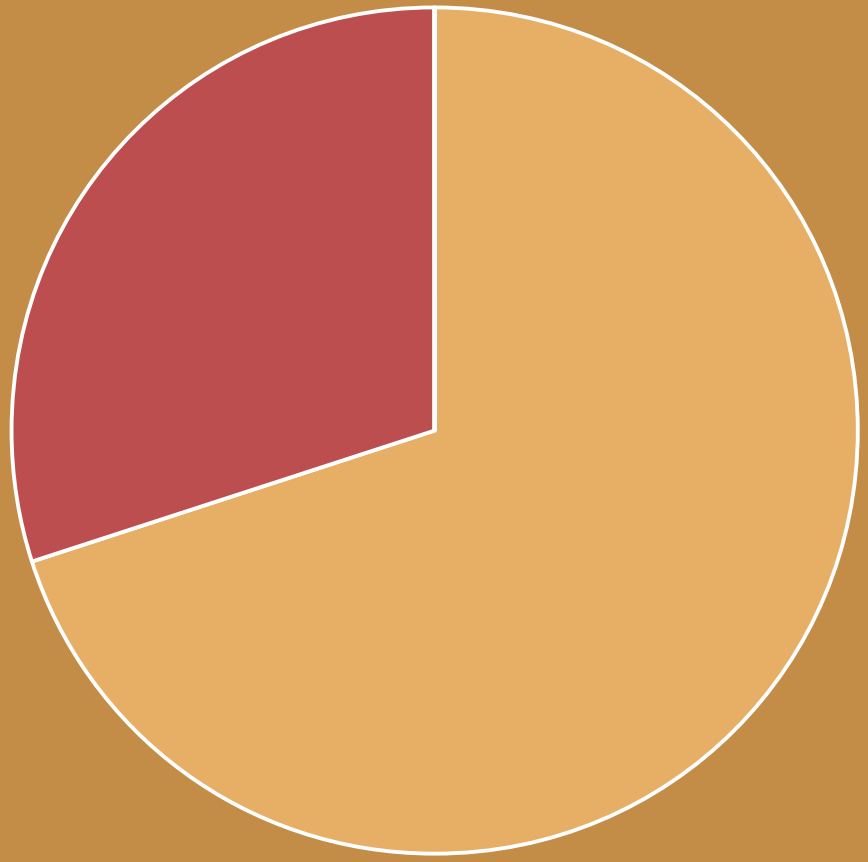
Hackers will craft a scenario for you to enter, in order to elicit a response which they believe will give them the result they are looking for.

Integrity

Types of Attacks & Real World Examples

Why talk about social engineering?

Social engineering is a component of the attack in nearly 1 of 3 successful data breaches, and it’s on the rise.



Source: 2016 Verizon Data Breach Investigation Report

Integrity

5 Common Attack Methods

DUMPSTER DIVING

PRETEXTING

PHISHING

PHYSICAL ENTRY

ENTICEMENT

Dumpster Diving

If not properly discarded, sensitive information may be discovered by hackers in waste receptacles and dumpsters.

- Printed emails, expense reports, credit card receipts, etc.
- Network or application diagrams, device inventory with IP addressing, etc.
- Notebooks, binders or other work papers containing sensitive information

Pretexting

- Fraudulent phone calls
- Used to extract information
- Also used to setup other attacks such as facility entry or phishing

Integrity

Phishing

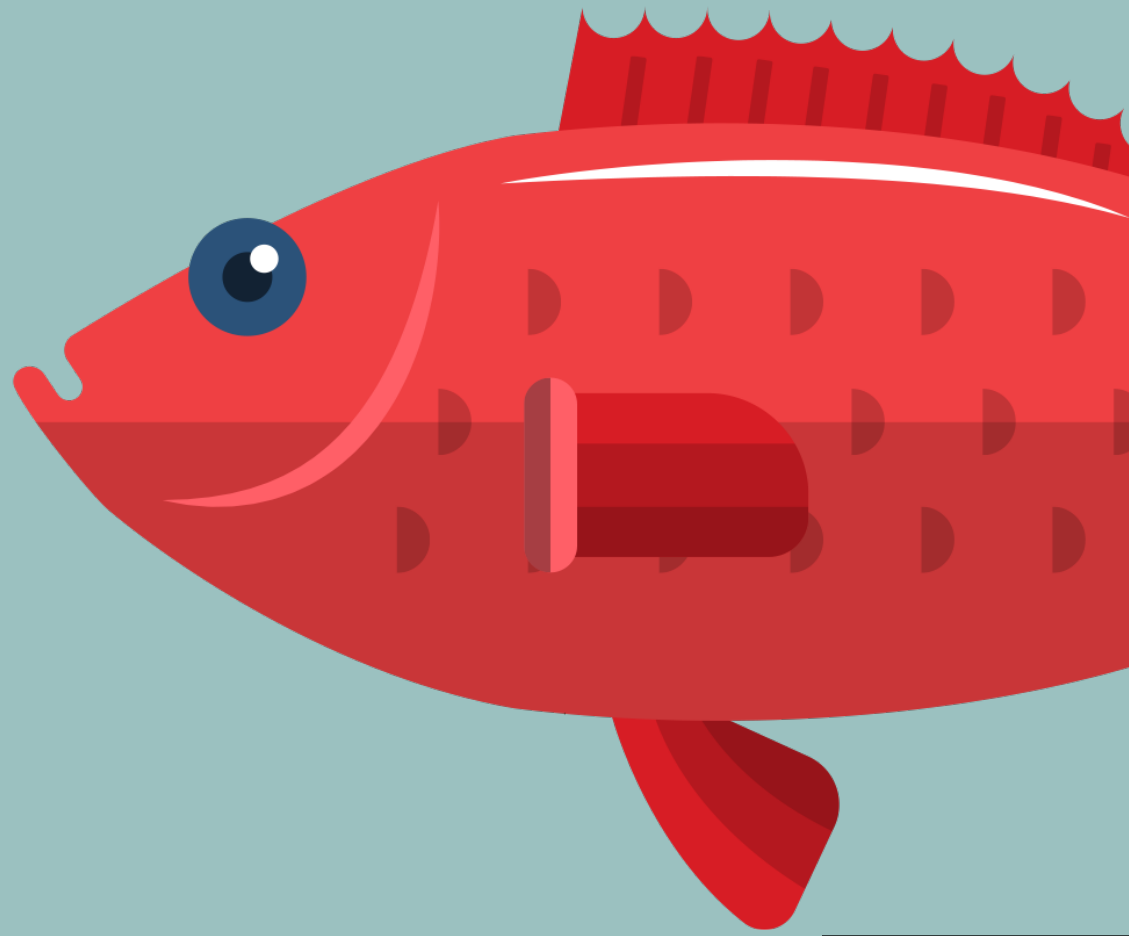
Phishing is the process of crafting emails that appear to be from a trusted source and typically invite the recipient to either supply confidential information or click on a malicious link or attachment.

Integrity

Phishing...

Tips For Identifying Phishing Attempts

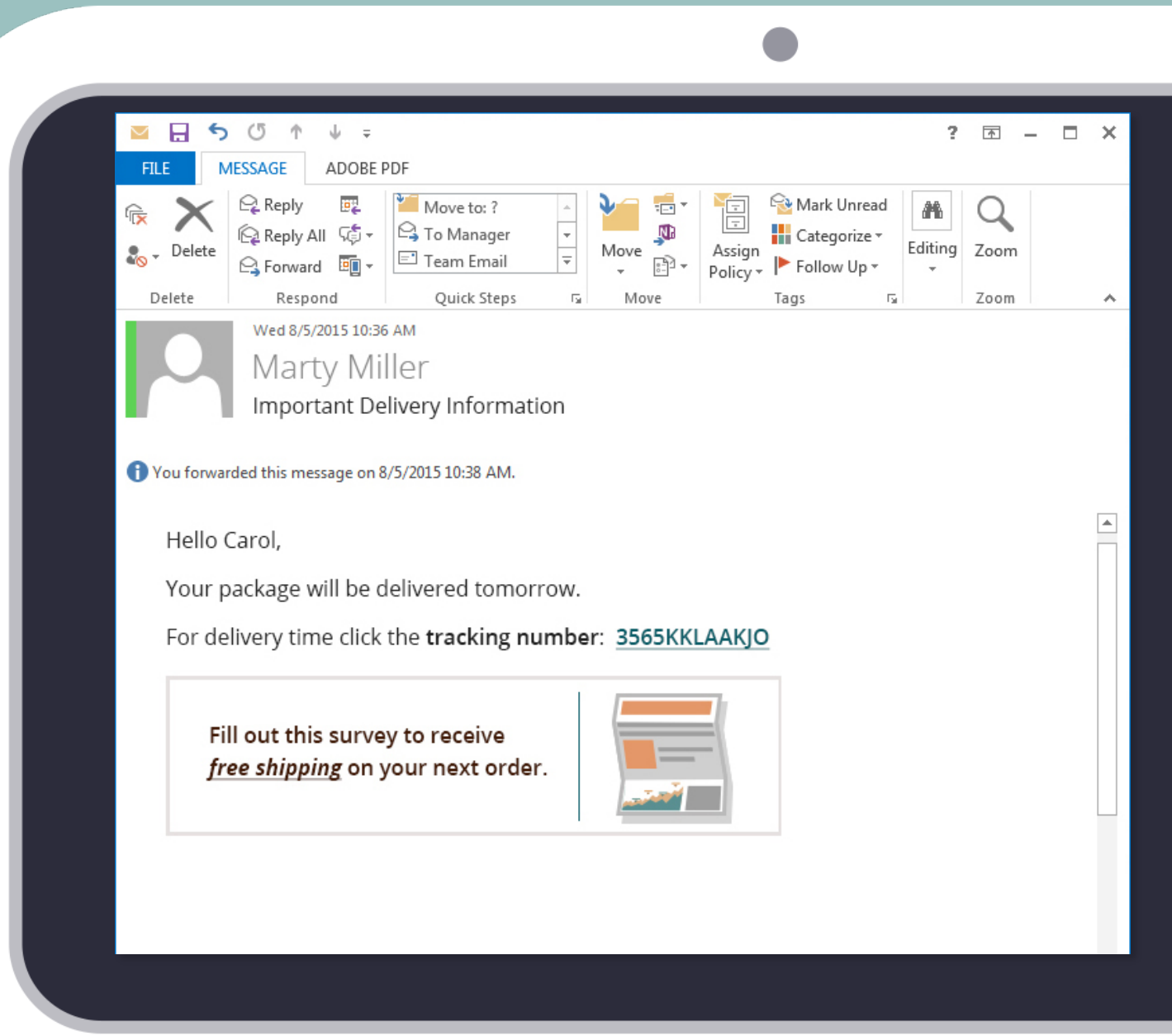
- The email asks you to update account information
- There are unfamiliar layouts/designs with no verification images
- The email provides unfamiliar hyperlinks



Integrity

Common Bait

- "Sweet Deals"
  - Free Stuff
  - Limited Time Offers
  - Package Delivery
- Help Me, Help You!
  - Tech Support
- You Gotta' See This!



Integrity

Facility Access

Hackers may rely on a physical approach to complement their technical attacks.

Integrity

Facility Access - *Example*

- **Piggy backing**: A hacker's method of entering a facility with a group of employees or maintenance workers
  - **Identifying unsecure areas**: Hackers search for loading docks, maintenance entrances, designated smoking areas or other locations that may not be well secured.

Act like you belong. If you believe it, so will everyone else.

Enticement - *Example*

A folder with enticing title/label left on ground outside an employee entrance with a USB thumb drive taped inside.

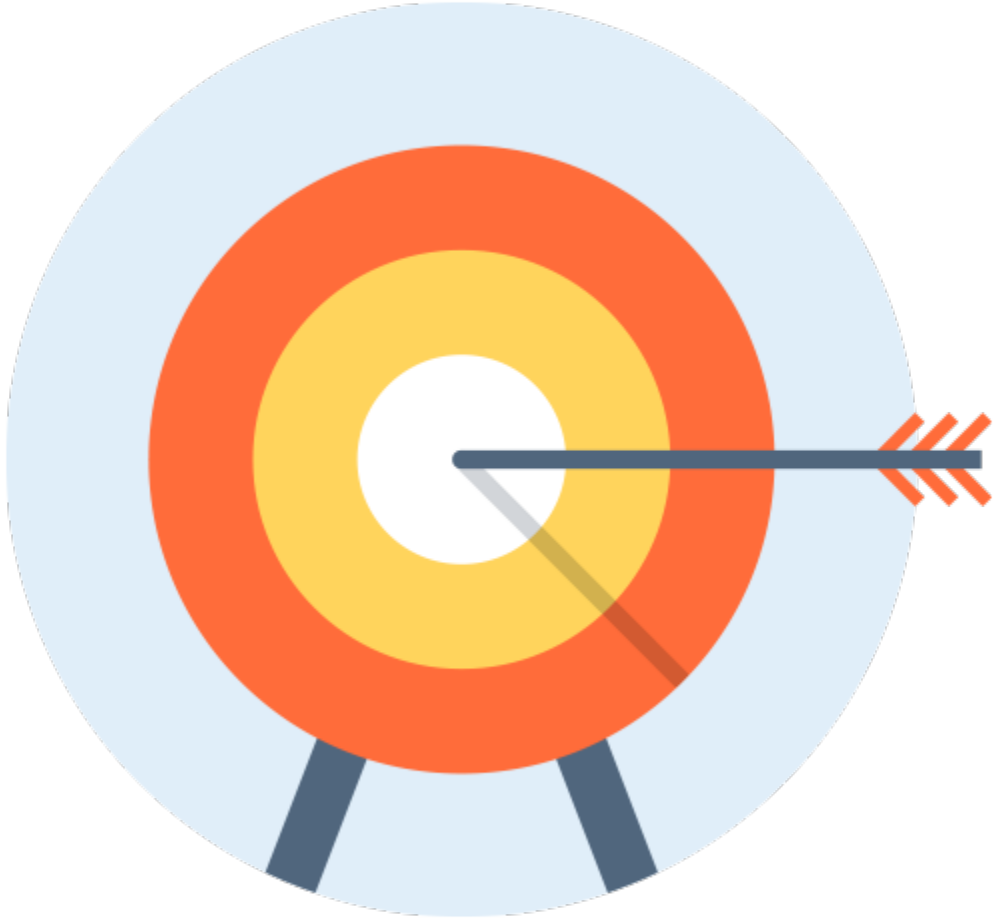
- USB, CD or DVDs left in conspicuous spaces
- May be accompanied by fake paper files
- Curiosity beats caution

Best Defenses

Integrity

Putting It All Together

- Targeted attacks will always use some form of social engineering
- Just like in military operations, intel makes or breaks a mission
- Hackers may never even need to use sophisticated technical attacks if you provide the information willingly



Don’t Fall for The Long Con

- Social engineering is nothing more than a con-game.
- The old “Long Con” has been ported to the digital world.
- Good cons are hard to spot.

Helpful Tips

- Enforce a strong paper destruction process
- Limit facility ingress/egress points
- Challenge unknown people in secure areas
- Implement technology to screen email and websites for attacks

Employee Training

- Prepare for different learning styles (audio, visual, hands-on)
- Engage the employee; make a personal plea
- Use gamification to enhance learning
- Awareness is not training, and training is not awareness

Program Validation

- Social engineering testing engagements provide assessments of how well your people, process, and technology are functioning.

Summary

- Social engineering is here to stay and it’s growing
- Your organization will suffer a data breach due to social engineering
- The study of human behavior has been used by criminals for centuries, cybercriminals are no different
- Employees must be trained to spot social engineering and how to react

For more information, connect with us online or with a phone call.

www.integritysrc.com/blog
@IntegritySRC
515-965-3756