Recognizing Cyber Threats



TEXAS A&M ENGINEERING

TEEX

EXTENSION SERVICE

Why Are We Here?

To gain a better understanding of how targeted cyber attacks occur, and how to respond to and recover from targeted cyber attacks.



Types of Cyber Attacks

Types of Cyber Attacks

- Untargeted Attacks
- **Targeted Attacks**

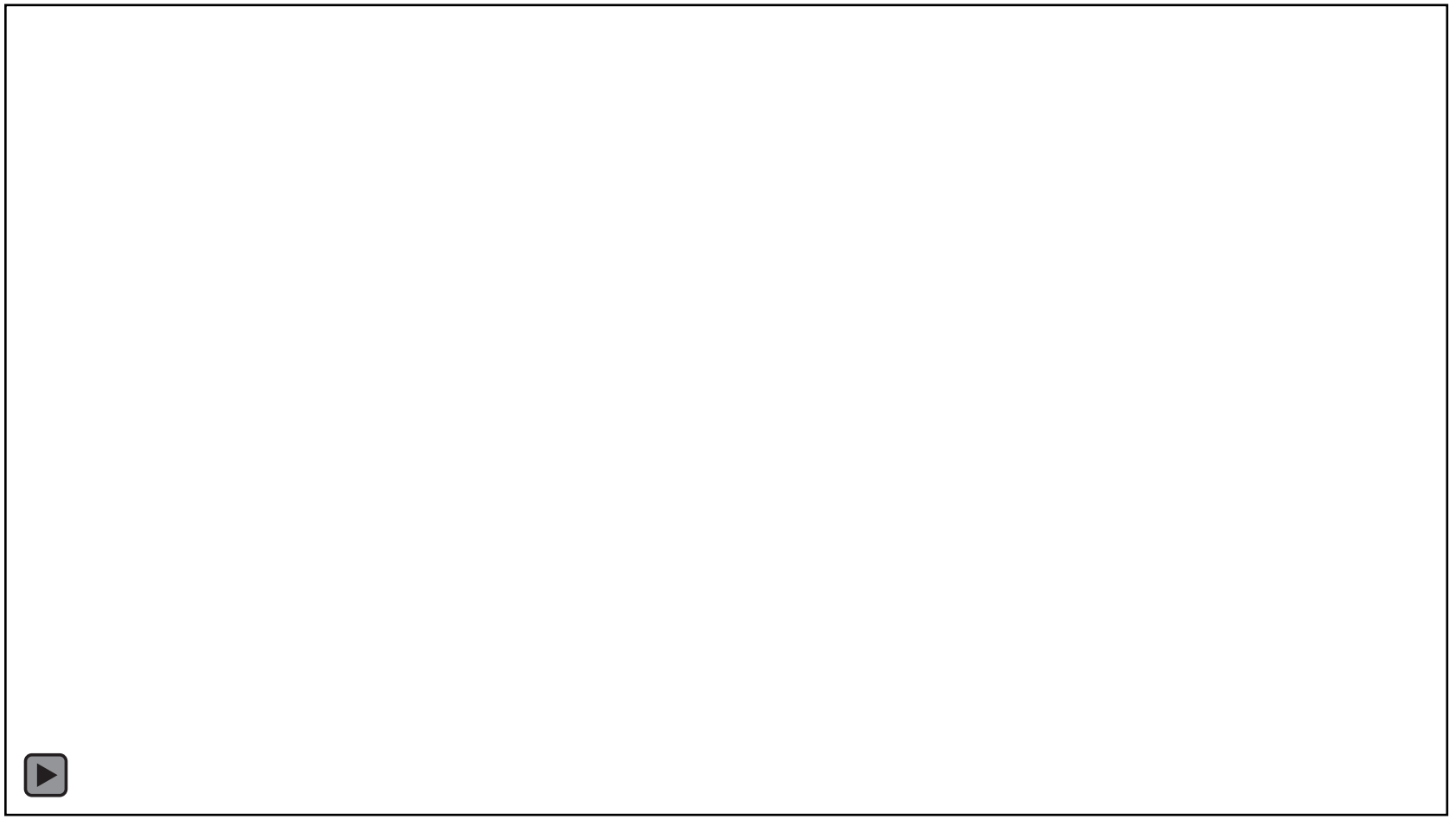


Targeted Attacks

- Specific
- Methods:
  - Malware
  - Ransomware
  - Phishing/SMShishing/Vishing
  - Public Wi-fi
  - Social Engineering
  - Botnets
  - Denial of Service (DoS)
  - Zero-Day Exploits



Phishing



Texas A&M Engineering
TEEX
EXTENSION SERVICE

Phishing

Email Spoofing

Email spoofing is the fabrication of an email header in the hopes of duping the recipient into thinking the email originated from someone or somewhere other than the intended source.

- Display Name Spoofing
- Domain Spoofing
- Close Cousin Spoofing

Phishing

Email Spoofing

Display Name Spoofing

The sender's name is usually displayed but the email address is not. This is almost always the case on *mobile devices*.

Ex: Jeffery Jordan (displayed name)
xyz@hackerrip.org

Phishing

Email Spoofing

Domain Spoofing

Phishing email that appears to come from a legitimate domain.

Ex: support@wells-fargo.com
support@apple-support.com
John.smith@bankofamerica.support.com

Phishing

Email Spoofing

Close Cousin

Hacking trick sends a domain name that is close to or even indistinguishable from the real domain.

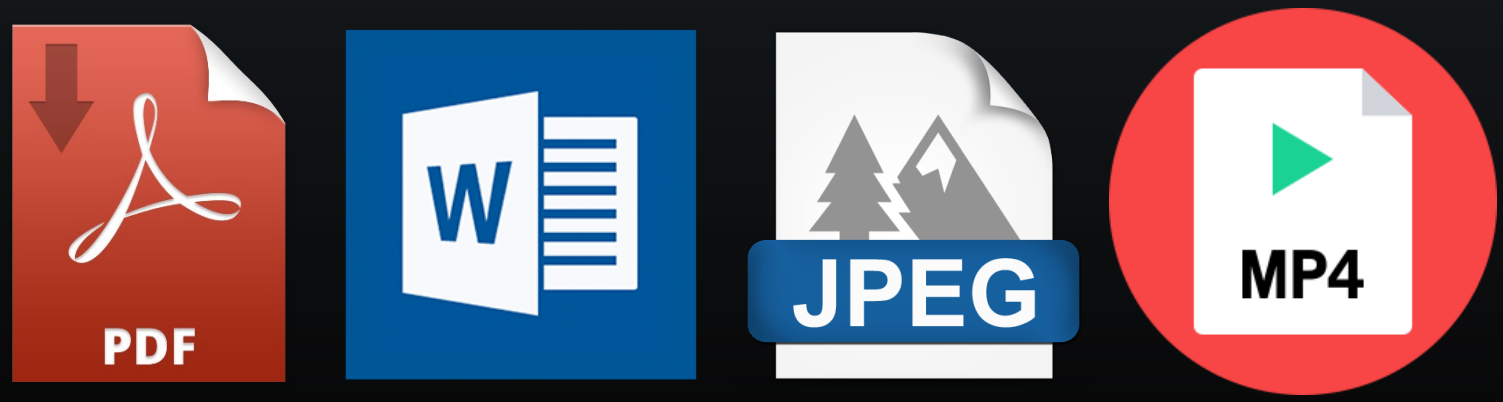
Ex: www.bofa.com (Bank of America)
www.apple-support.com
www.NIS.tamu.com
www.apple.co

Phishing

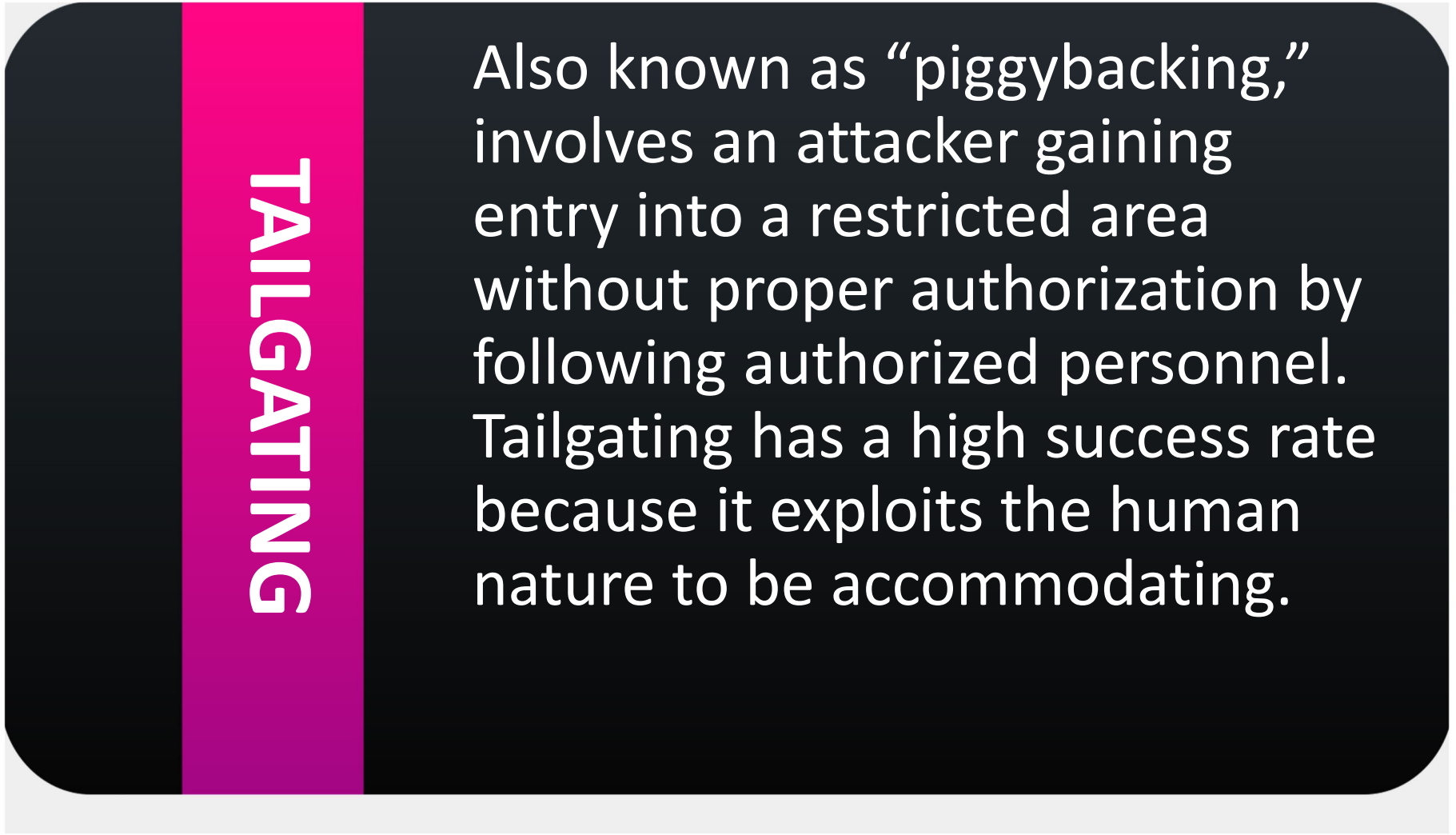
Email Spoofing

Attachment Phishing

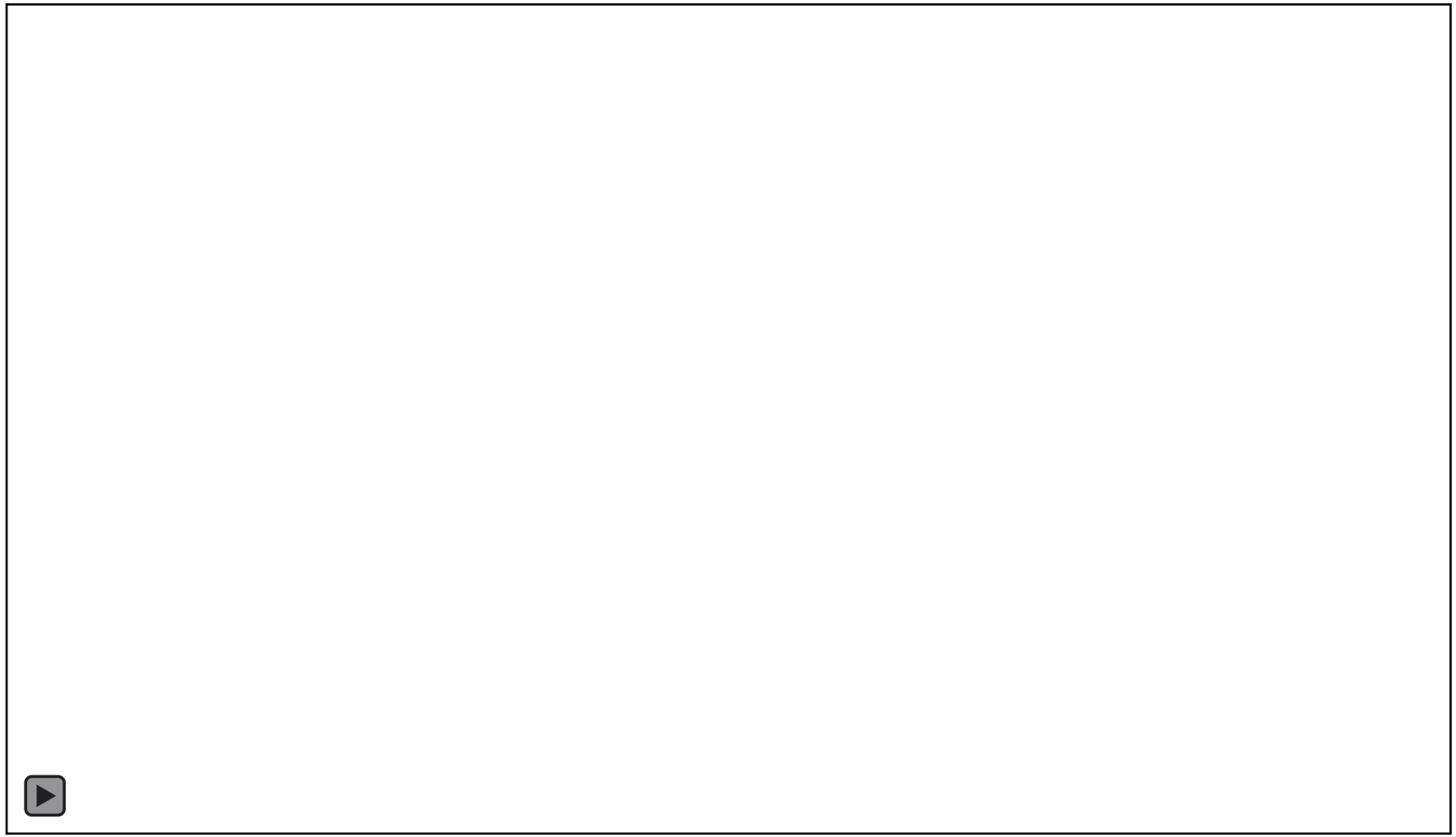
To avoid detection by email filters, phishing links can be attached to docs, such as PDF, Word, JPEG, etc.



Tailgating


TAILGATING
Also known as “piggybacking,” involves an attacker gaining entry into a restricted area without proper authorization by following authorized personnel. Tailgating has a high success rate because it exploits the human nature to be accommodating.

Public WiFi



Texas A&M Engineering
TEEX
EXTENSION SERVICE

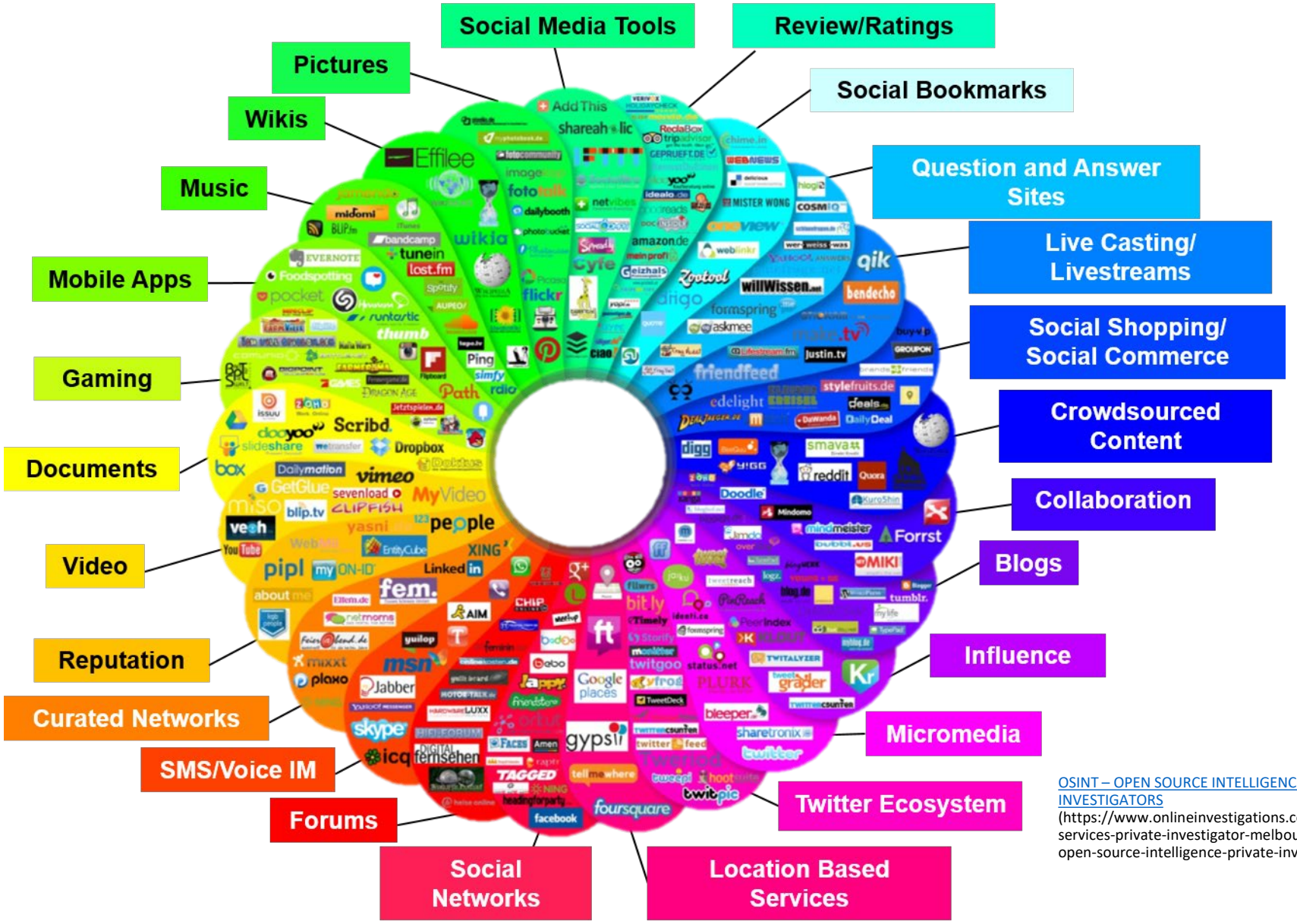
Social Engineering

- The practice of obtaining confidential information by manipulation of legitimate users
  - Email
  - Telephone
  - Face-to-Face
  - Shoulder Surfing
  - Dumpster diving
  - Spear Phishing/ Smishing/ Vishing
    - Whaling
  - Insider Threat
  - Social Networking



TEXAS A&M ENGINEERING TEEX EXTENSION SERVICE

Open Source Intelligence

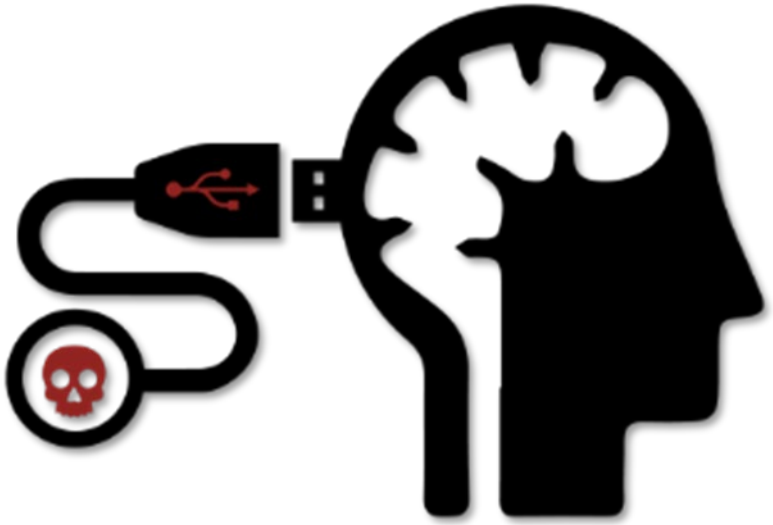


OSINT – OPEN SOURCE INTELLIGENCE PRIVATE INVESTIGATORS
(https://www.onlineinvestigations.com.au/our-services-private-investigator-melbourne/osint-open-source-intelligence-private-investigators/)

TEXAS A&M ENGINEERING
TEEX
EXTENSION SERVICE

Example of a Cyber Attack

Neuro-Linguistic Hacking



Face-to-face social engineering using psychological manipulation to gain someone's trust and obtain information.

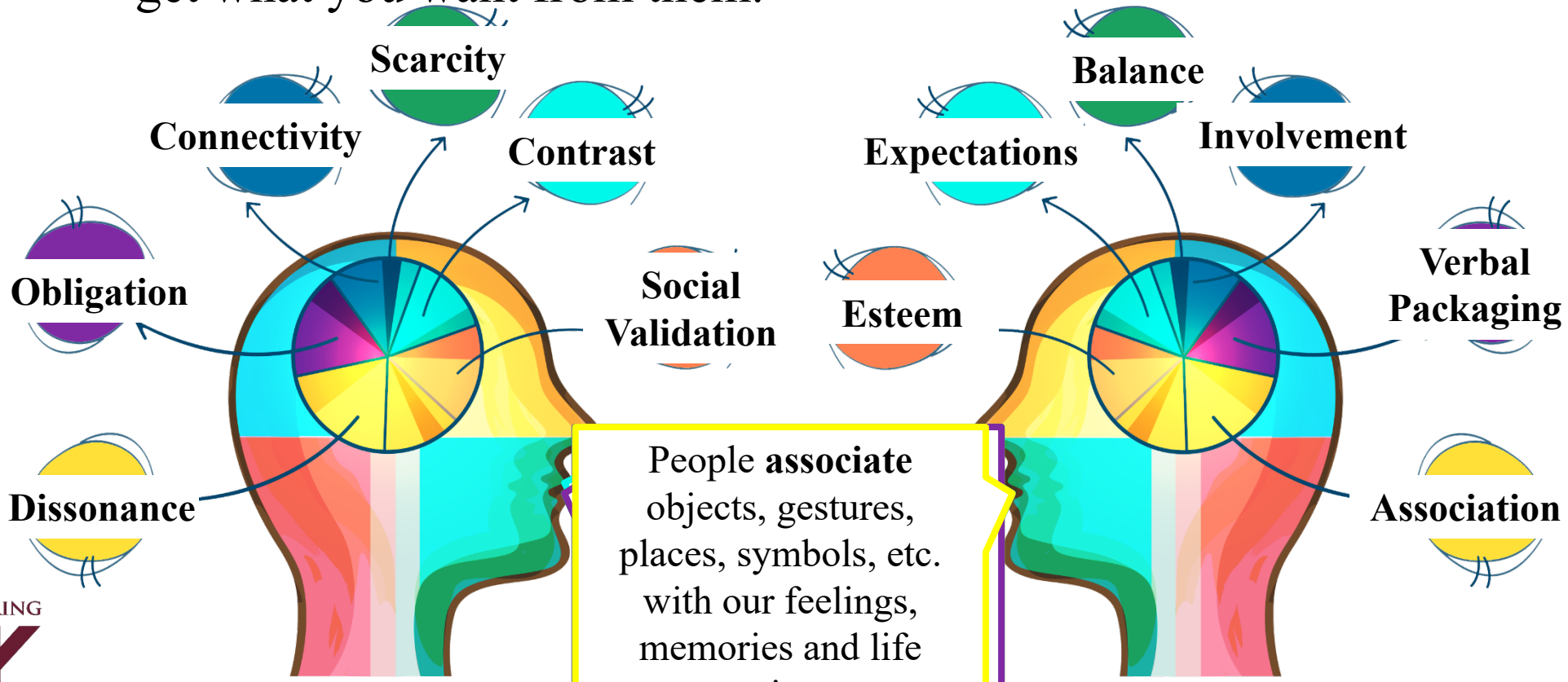
Hacking a person is easier and less time consuming than hacking a computer system.

TEXAS A&M ENGINEERING
TEEX
EXTENSION SERVICE

Neuro-Linguistic Hacking

12 Laws of Neuro-Linguistic Programming

An approach to interacting with people that enables you to get what you want from them.



TEXAS A&M ENGINEERING TEEX EXTENSION SERVICE

Neuro-Linguistic Hacking

Big Five/Ocean Personalities



Openness



Conscientiousness



Extraversion



Agreeableness



Neuroticism

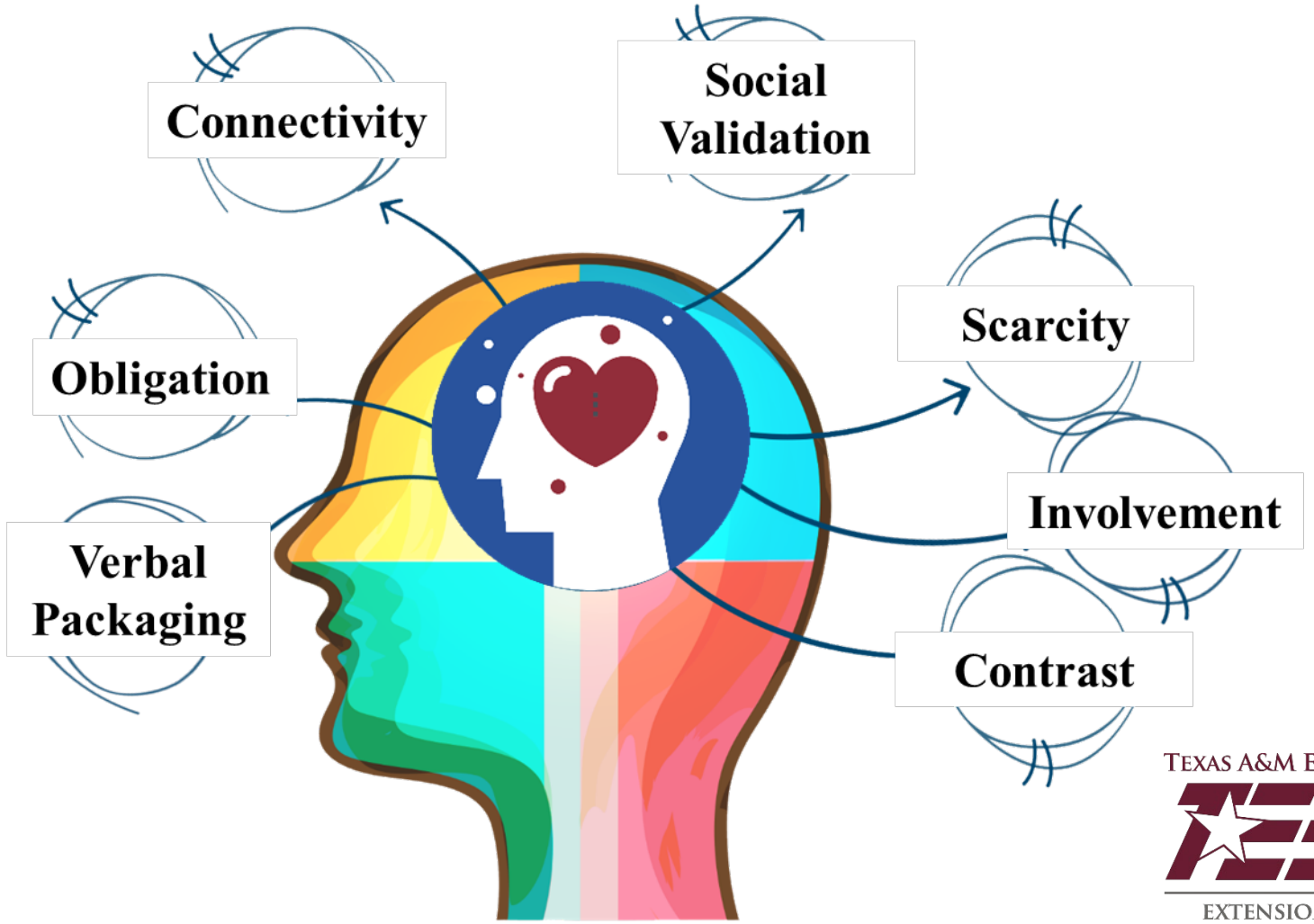
TEXAS A&M ENGINEERING
TEEX
EXTENSION SERVICE

Neuro-Linguistic Hacking

Oceans Personality Types
and Neuro-Linguistic Programming

Openness

- Open-minded
- Receptive to new things
- Adventurous
- Creative
- Love of learning



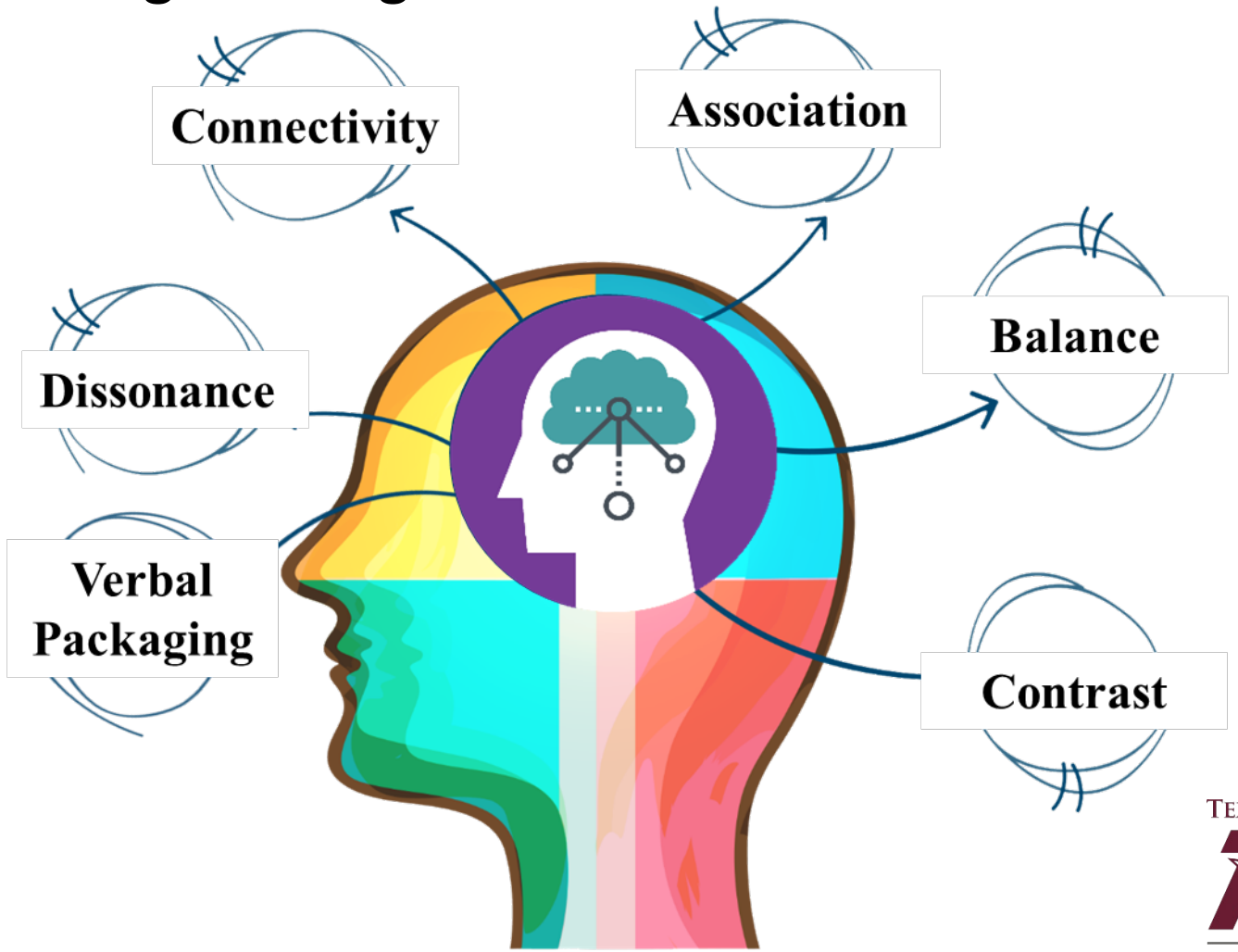
TEXAS A&M ENGINEERING
TEEX
EXTENSION SERVICE

Neuro-Linguistic Hacking

Oceans Personality Types
and Neuro-Linguistic Programming

Conscientiousness

- Want to do what is right
- Honor commitments
- Responsible
- Reliable



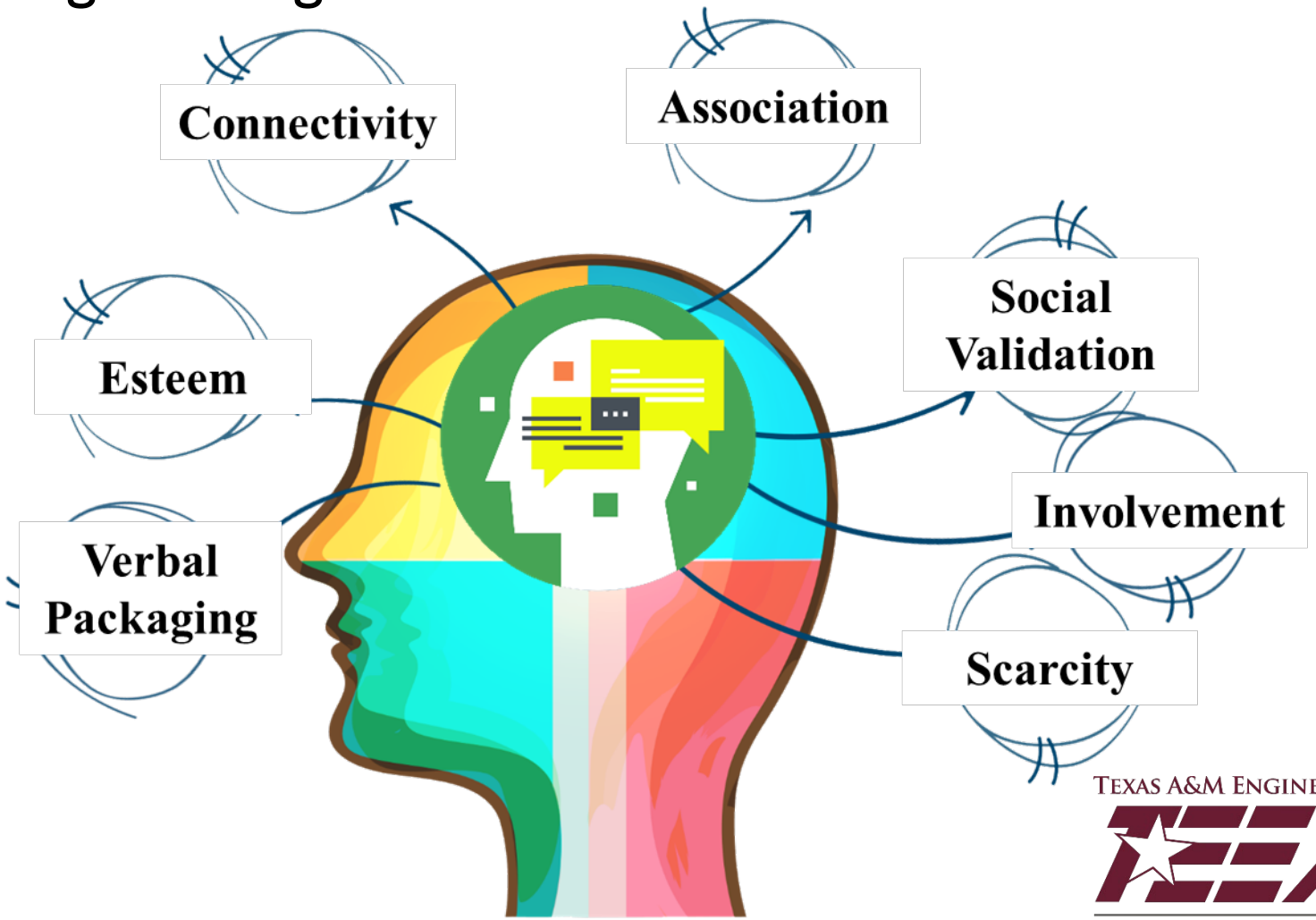
TEXAS A&M ENGINEERING
TEEX
EXTENSION SERVICE

Neuro-Linguistic Hacking

Oceans Personality Types
and Neuro-Linguistic Programming

Extraversion

- Outgoing
- Friendly
- Helpful
- Attention-seeking
- Love social interaction



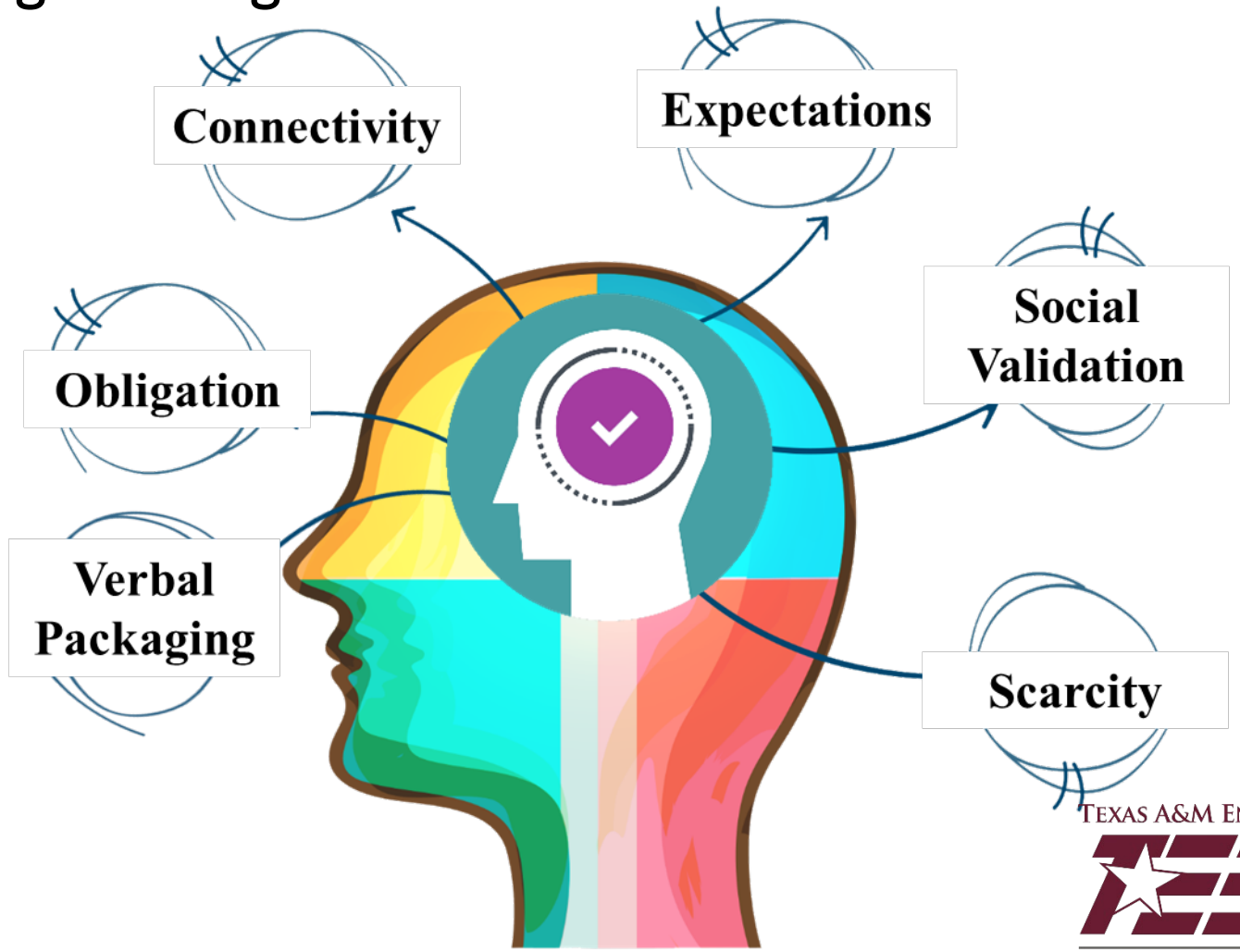
TEXAS A&M ENGINEERING
TEEX
EXTENSION SERVICE

Neuro-Linguistic Hacking

Oceans Personality Types
and Neuro-Linguistic Programming

Agreeableness

- Helpful
- Cooperative
- Trusting
- Empathetic
- Like to avoid conflict



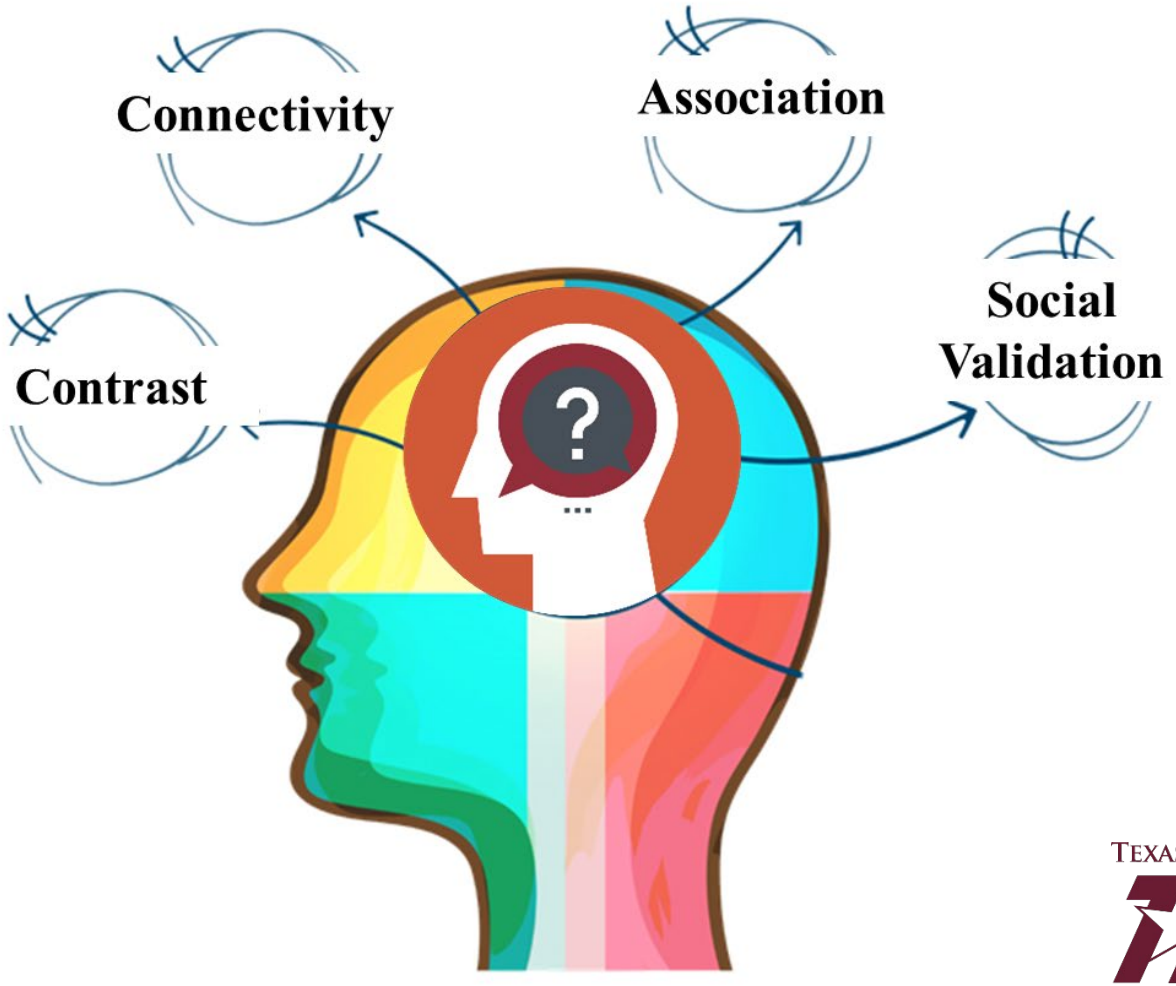
TEXAS A&M ENGINEERING
TEEX
EXTENSION SERVICE

Neuro-Linguistic Hacking

Oceans Personality Types
and Neuro-Linguistic Programming

Neuroticism

- Skeptical
- Moody
- Negative
- Experience more stress
- Worry a lot



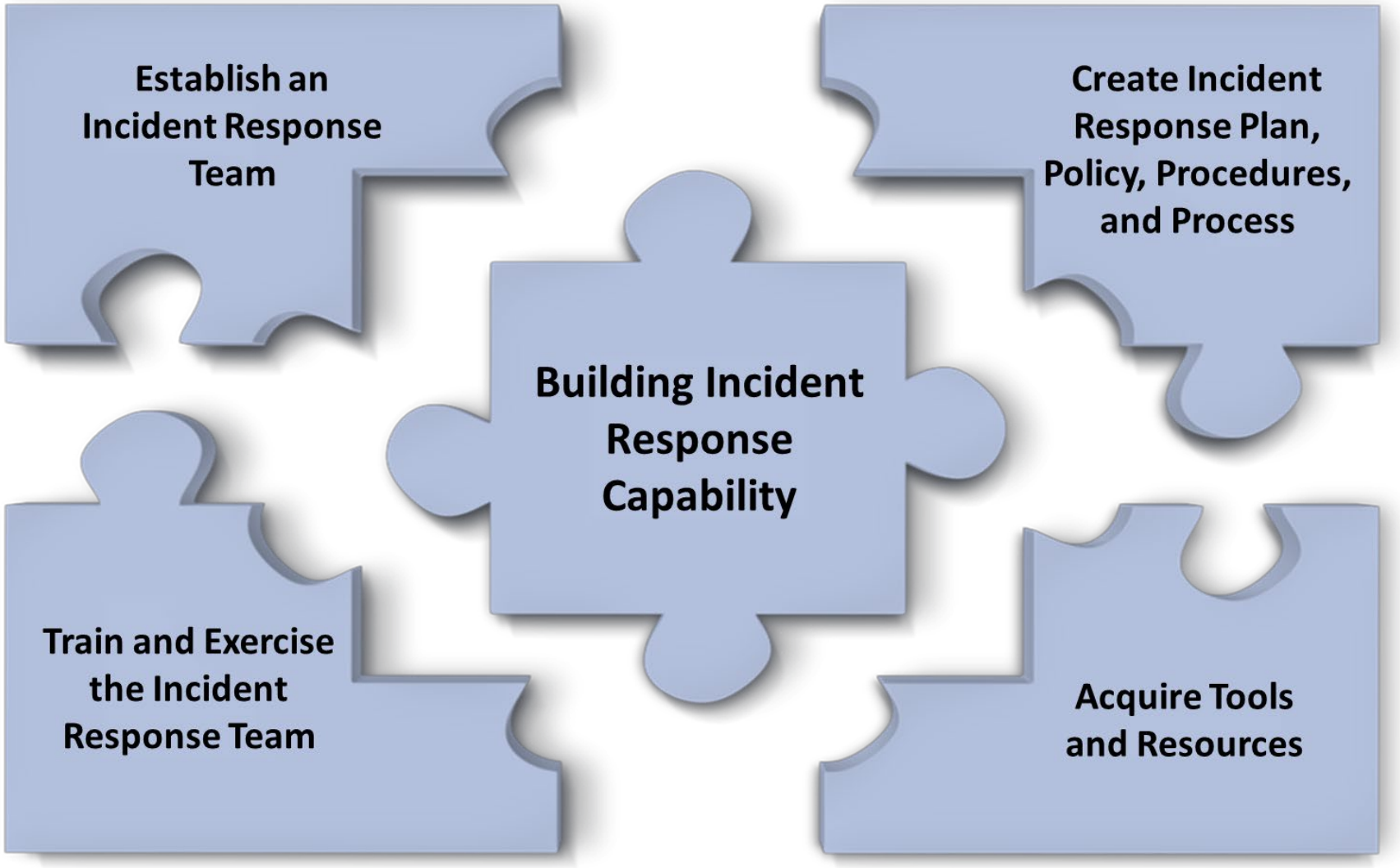
TEXAS A&M ENGINEERING
TEEX
EXTENSION SERVICE

Defense



TEXAS A&M ENGINEERING
TEEX
EXTENSION SERVICE

Defense



TEXAS A&M ENGINEERING
TEEX
EXTENSION SERVICE

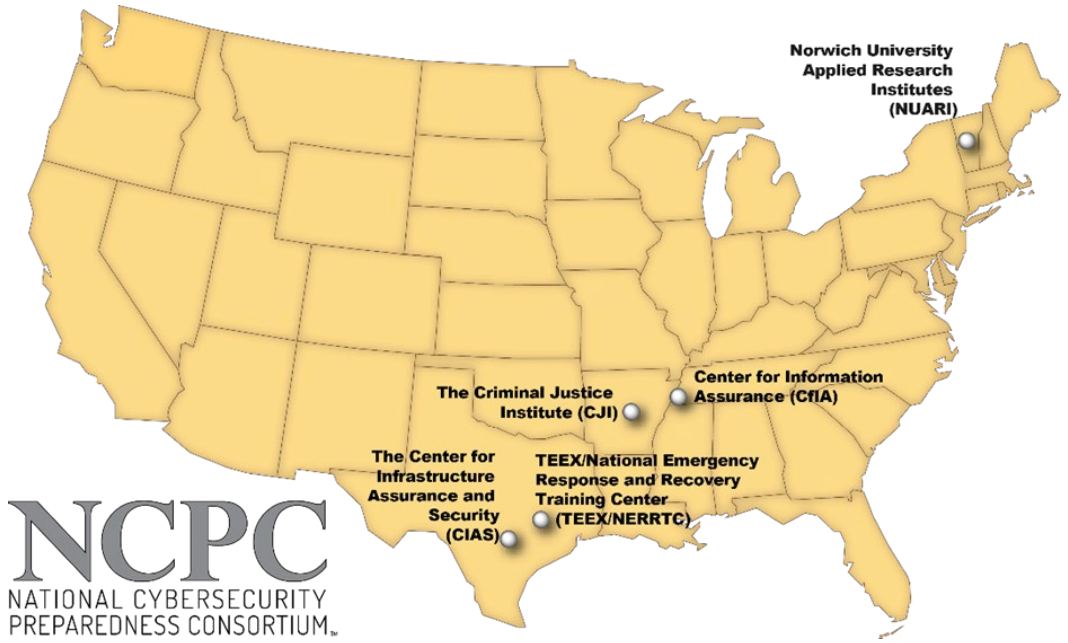
FEMA Funded Cybersecurity Training Resources



NCPC Members

- Cyber Defense Initiative – Criminal Justice Institute/University of Arkansas System
  - Dr. Cheryl May, Consortium Chair
- Center for Infrastructure Assurance and Security, University of Texas-San Antonio
- National Emergency Response and Recovery Training Center, Texas A&M Engineering Extension Service
- Norwich University Applied Research Institutes, Norwich University
- Center for Information Assurance, University of Memphis

NCPC
National Cybersecurity Preparedness Consortium



FEMA

National Training and Education Division
(https://www.firstrespondertraining.gov/frts/)

National Cybersecurity Preparedness Consortium
(https://www.nationalcpc.org/)

NCPC Overview

NCPC Mission

To help State, Local, Tribe and Territory (SLTT) governments establish viable and sustainable cybersecurity programs to prevent, detect, respond to, and recover from cyber attacks.

FEMA Certified Course Portfolio

51 FEMA certified cybersecurity courses

- 23 instructor-led and 28 web-based
- 18 additional courses in development
- Over 120,000 trained nationally to date

Training Categories

Courses designed to fill training needs in multiple topic areas:

- Awareness
- Coordination and Planning
- Incident Response and Recovery
- Information Sharing
- Technical

Target Audience

Courses designed to meet the needs audiences at multiple levels:

- End-Users
- Information Technology Personnel
- Leadership / Management

FEMA

National Training and Education Division
(https://www.firstrespondertraining.gov/frts/)

National Cybersecurity Preparedness Consortium
(https://www.nationalcpc.org/)

Awareness

- **AWR-136 – Essentials of Community Cybersecurity (Length – 4 hours)**
  This discussion-based, non-technical course is an introduction to cybersecurity provides individuals, community leaders, and first responders with information on how cyber attacks can impact, prevent, and/or stop operations and emergency responses in a community.
- **AWR-376 – Understanding Social Engineering Attacks (Length – 8 hours)**
  This web-based course focuses on the idea that preventing social engineering attacks not only requires comprehensive security measures, but also significant understanding and awareness as to how such attacks can exploit human online behaviors.
- **AWR-385-W – Mobile Device and Security (Length – 6.5 hours)**
  This web-based course provides an understanding of the history, definitions, and components that make up the Internet of Things (IoT) and addresses the different applications of IoT as well as applicable laws and policies, technologies, emerging threats, best practices, security, and a variety of existing and developing technologies.
- **AWR-402-W – Introduction to Internet of Things (IoT) (Length – 2 hours)**
  This web-based course provides an understanding of the history, definitions, and components that make up the Internet of Things (IoT) and addresses the different applications of IoT as well as applicable laws and policies, technologies, emerging threats, best practices, security, and a variety of existing and developing technologies.

Cyber Incident Response and Recovery

- **PER-371 - Cybersecurity Incident Response for IT Personnel (Length – 24 hours)**
  This course is designed to address the gap in specific technical skills needed for an effective cyber response and uses a mobile cybersecurity range for students to apply what they have learned about cybersecurity theories and work in groups to defend a network against simulated attacks.
- **MGT-456 - Integration of Cybersecurity Personnel into the Emergency Operations Center (EOC) for Cyber Incidents (Length – 24 hours)**
  This course is designed to assist jurisdictions with coordinating and managing response efforts between emergency response organizations and critical infrastructure cybersecurity personnel.
- **AWR-389-W - Incident Response for Municipal, Police, Fire and EMS Information Technology Personnel (Length – 2 hours)**
  This web-based course introduces the basics of the incident response process to the Information Technology personnel in Police, Fire or EMS departments.
- **MGT-465 – Recovering from Cybersecurity Incidents (Length – 16 hours)**
  This course encourages collaboration efforts among individuals and organizations responsible for both physical and cybersecurity toward development of integrated risk management strategies that lead to enhanced capabilities necessary for the protection of our nation's critical infrastructure.

FEMA

Technical

- **PER-256 - Comprehensive Cybersecurity Defense (CCD) (Length – 32 hours)**
  A basic-level course designed for technical personnel who monitor and protect our nation's critical cyber infrastructure.
- **PER-257 - Cybersecurity First Responder (CFR) (Length – 32 hours)**
  An intermediate-level course designed for technical personnel who are first responders to any type of cyber-based attack against our nation's critical cyber infrastructure.
- **AWR-368-W - Introduction to Basic Vulnerability Assessment Skills (Length – 12 hours)**
  An introductory course intended to help prepare learners for the technical challenges associated with conducting vulnerability assessments and/or penetration testing.
- **PER-398 – Cybersecurity Resiliency in Industrial Control Systems (Length – 8 hours)**
  An intermediate-level course designed to enhance understanding of the critical nature of Industrial Control System environments and the associated risks, threats, and defenses within an organization, business, or government entity.

Information Sharing

- **AWR-381-W - Establishing an Information Sharing and Analysis Organization (Length – 8 hours)**
  This web-based course will assist communities of interest to establish an Information Sharing and Analysis Organization (ISAO).
- **MGT-473 - Organizational Information Sharing Integration (Length – 16 hours)**
  This two-day, instructor-led course is designed for mid-level management to address information sharing as an emerging national priority. State, Local, Tribes and Territories (SLTTs) will understand how to integrate cyber threat information sharing into their information sharing practices.
- **AWR-398-W - Introduction to ISAOs (Length – 2 hours)**
  This web-based course is an introduction to Information Sharing and Analysis Organizations (ISAOs) that also covers the basics of the cybersecurity information sharing processes.

Latest NCPC Courses – Certified and Coming Soon

NCPC
National Cybersecurity Preparedness Consortium

Web-Based

- AWR-399-W – Detecting and Responding to a Cyber Attack
- AWR-402-W – Introduction to Internet of Things (IoT) Devices
- AWR-403-W – Examining Advanced Persistent Threats

Coming Soon:

- AWR-431-W – Remote/Home-Office Cybersecurity Preparedness

Instructor-Led

- AWR-421 – Demystifying Cyber Attacks
- PER-412 – Cyber Threat Intelligence
- MGT-478 – Community Cybersecurity Information Sharing Integration

Coming Soon:

- PER-TBD – Network Traffic Analysis

FEMA

National Training and Education Division
(https://www.firstrespondertraining.gov/frts/)

National Cybersecurity Preparedness Consortium
(https://www.nationalcpc.org/)

For More Information:

Scheduling or Accessing Training

Information on these courses and more is available on the DHS/FEMA/NTED website (https://www.firstrespondertraining.gov/frts/)

All web-based cybersecurity courses are available for anyone to take (https://teex.org/program/nerrtc-online-training/)

FEMA