



**TEXAS RE**  
Ensuring electric reliability for Texans

# **Cybersecurity Threats**

**Jason Moehlman**  
**Principal, IT & Security Systems**

**August 5, 2025**

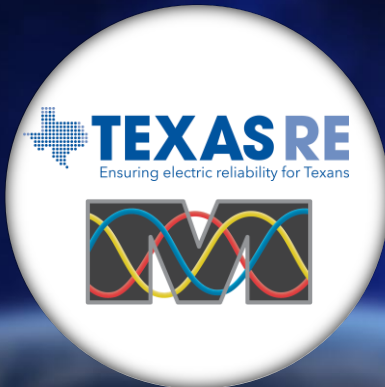
# Antitrust Admonition

**Texas Reliability Entity, Inc. (Texas RE) strictly prohibits persons participating in Texas RE activities from using their participation as a forum for engaging in practices or communications that violate antitrust laws. Texas RE has approved antitrust guidelines available on its website. If you believe that antitrust laws have been violated at a Texas RE meeting, or if you have any questions about the antitrust guidelines, please contact the Texas RE General Counsel.**

**Notice of this meeting was posted on the Texas RE website and this meeting is being held in public. Participants should keep in mind that the listening audience may include members of the press, representatives from various governmental authorities, and industry stakeholders.**



# Upcoming Texas RE Events



**August 12, 2025**  
**Modernization of  
Standards Processes  
and Procedures Task  
Force Webinar**



**August 19, 2025**  
**CIP-003-8**



**August 26, 2025**  
**Data Breach  
Response**



# Upcoming Texas RE Events



September 17, 2025

Q3 MRC and Board  
Meetings



October 1, 2025

Winter  
Weatherization  
Workshop



November 5, 2025

Fall Standards,  
Security, &  
Reliability  
Workshop



# Upcoming ERO Enterprise Events

**NERC**NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION**Date****Event****August 6****Protection System Workshop (RF)****August 7****Human Performance Workshop (RF)****August 12-14****Power System and Security Conference (WECC)****August 13****Inverter-Based Resource Webinar (MRO)**

slido

Product

Solutions

Pricing

Resources

Enterprise

Log In

Sign Up

## Joining as a participant?

# Enter event code

Join an existing event

#TXRE

The ultimate Q&A and polling platform

## Give a voice to your audience, wherever they are.

Create your own Slido event

[Watch a video](#) or [Schedule a demo](#)



# Cybersecurity Threats—Agenda

## Review the Last Year(ish) of Cyber Incidents/Events

- Typhoon Chain
- Crowdstrike
- DDoS Attacks
- North Korean Remote Worker Scheme

## Social Engineering

- Methods
- AI Risks
- Defenses



# Cybersecurity Threats—Typhoon Chain Threat



## Volt Typhoon

- Critical Infrastructure
- Persistence and Stealth

## Salt Typhoon

- Communications Infrastructure

## Silk Typhoon

- Supply Chain

# Cybersecurity Threats—Recent Incidents

## CrowdStrike Event

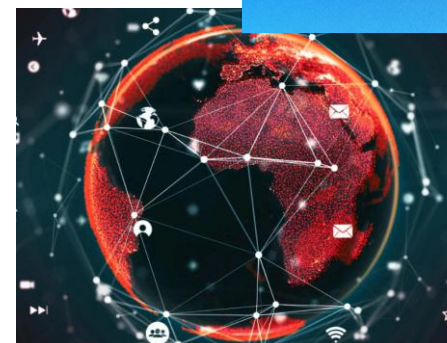
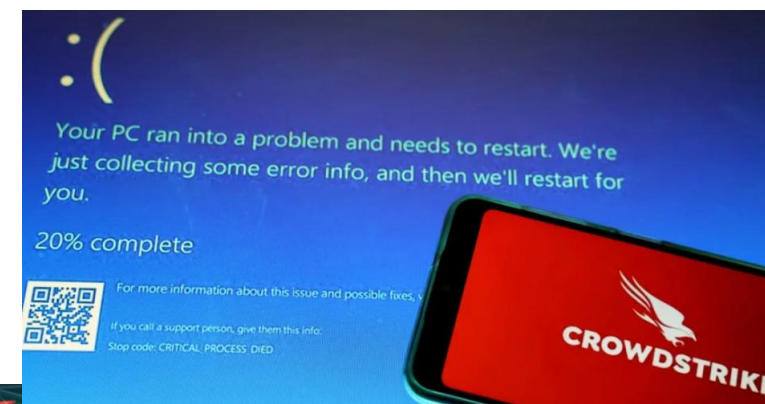
- “Channel File 291” Incident
- Windows Resiliency Initiative

## DDoS Attacks

- 358% Increase in Year-Over-Year Attacks
- Mirai Malware

## North Korean Remote Worker Scheme

- Laptop Farms



# Cybersecurity Threats—Social Engineering



## Goals

- Money
- Information
- Virtual and Physical Access

## Vectors

- Fear
- Trust
- Lack of Awareness
- Conflict Avoidance

## New Threat

- AI



# Social Engineering Tactics

Phishing

Spear Phishing/Whaling

Smishing (SMS Phishing)

Vishing (Voice Phishing)

Business Email  
Compromise (BEC)

Pretexting

Baiting

Tailgating/Piggybacking



# Social Engineering—Examples

## Phishing



### Password Expiration - Authentication Service

Hi User,

Password for your account will expire today. Please follow the link to update your account password.

Keep same Password

Support Service Desk Microsoft

Note: This verification is for it's intended receiver

# NETFLIX

### Automatic payment.

Hi Customer,

Your Auto payment cannot process.  
Your subscription period will end on Wed, January 22, 2020.

[Click Here](#) to update payment method

please update your payment methode for continue Netflix feature.

The Netflix Team

## Smishing

message  
Sunday 12:57 PM

Please pay for FastTrak Lane on December 22, 2024. In order to avoid excessive late fees and potential legal action on the bill, please pay the fee in time. Thank you for your cooperation and wish you a happy holiday.

<https://thetollroads.com-us>

(Please reply Y, then exit the text message and open it again to activate the link, your Safari browser)

7:27

Text Message  
Today 08:58

We have identified some unusual activity on your online banking. Please log in via <http://bit.do/dq3WJ> to secure your account.

Text Message  
Today 5:56 PM

Hello Olivia, your FEDEX package with tracking code GB-6412-GH83 is waiting for you to set delivery preferences: [e3fmr.info/onAyXsVfomA](http://e3fmr.info/onAyXsVfomA)



# Social Engineering—AI Powered

## How is AI Altering the Social Engineering Environment?

- AI speeds and scales social engineering
- Specialized AI models (WormGPT, FraudGPT) can generate well-written, believable, and tailored phishing emails
  - One study showed a 54% increase in clicked emails
- Volume
  - Thousands of emails can be created and sent in minutes
- Personalization
  - Public data, social media
- Realism
  - Deepfakes & cloned voices
- Adaptability
  - Real-time chatbots



# Social Engineering—AI Phishing Scenario

## Reconnaissance

AI algorithms scour publicly available information like social media profiles, corporate websites, and news articles to gather details about individuals and organizations.

## Content Generation

Using this information, AI-powered text generation tools create highly customized and believable phishing emails. They can mimic the writing style and tone of trusted contacts, incorporate references to recent activities or projects, and use accurate terminology and formatting, making the emails appear legitimate.

## Attack and Automate

Send emails and adjust for success—automated A/B testing can be used to optimize subject lines, email structures, and content variations for maximum impact.



# Social Engineering—AI Deepfake Voice Phishing

- **Vishing attacks surged almost 500% in 2024**
- **Voices can be cloned with 3-5 minutes of sample audio**
- **Mostly used for fraud but expanding to political and other purposes**
- **AI-powered tools generate personalized and believable audio**

## **AI-generated voice messages posing as Secretary of State Marco Rubio**

- Two voicemails and text message sent over the Signal app
- Messages sent to U.S. and foreign officials

## **\$25M loss to deep fake scheme**

- Finance member joined a video conference call with people he believed to be the chief finance officer and other employees
- Was convinced to wire money to fraudsters

## **Florida mother loses \$15K to deep fake voice call**

- Received phone call from a number that looked like her daughter's
- Voice that she believed was her daughter claiming to be in jail and needing money for bail



# Social Engineering—Workplace Defenses

- **Training**
  - Awareness training, phishing tests, simulated attempts
- **Multifactor Authentication**
- **Conditional Access Policies**
- **SPF, DKIM, DMARC**
  - Check for sender's address, spoofed links, suspicious attachment
- **Finance Change Control**
- **Social Media Policies**
- **Application Control, Attack Surface Reduction Policies**
- **Deepfake Detection Tools**
- **Zero Trust**



# Social Engineering—Personal Defenses

**Be Skeptical!**

**If Urgency is  
Implied,  
SLOW DOWN**

## **Password Control**

- Password manager
- Enable MFA anywhere you can

**Keep Devices  
Patched**

**Limit What You  
Share Online**

**Freeze Your Credit**

**Socialize  
Awareness**



# Social Engineering—Key Takeaways

## AI Speeds and Scales Social Engineering

- Right now, not containable
- Voice/video deepfakes are already causing multi-million-dollar frauds

## Multifaceted Approach to Defense

- Be proactive
- Vigilance
- Advanced technological defenses

## Only You



The background of the slide features a blurred image of the Texas state flag on the left and a close-up of a wind turbine's hub and blades on the right. The blades are white with red tips. A dark blue rounded rectangle is centered over the image.

# Questions?



**TEXAS RE**

Ensuring electric reliability for Texans