CySER 2026

Human Behavior and Organizational Security

Robert Crossler

Washington State University

DEEPFAKES & SECURITY BYPASS

AI-Enhanced Threats

- AI-cloned voices impersonate executives
- Live video deepfakes bypass visual checks
- Help desks manipulated by convincing calls
- Finance teams pressured by fake authority

Stronger Verification

- Multi-channel identity confirmation
- Code word or challenge systems
- Policies that override instinctive trust
- Regular deepfake awareness training

Discussion: *If a deepfake call appeared to come from a senior leader asking for urgent access, what process should override instinctive trust?*

INCIDENT OVERVIEW

The Canvas Compromise

What Happened

Data Exposed

Attack Vector

Attribution

Which details are confirmed vs. attacker claims?

DISCUSSION PROMPTS

Why do attackers target centralized systems like learning management platforms?

How does partial data exposure still create significant downstream risk?

What makes voice-based impersonation more convincing than email?

What verification step could stop a social engineering attempt early?

How should organizations respond when threat actor claims exceed confirmed reports?

THE VISHING HYPOTHESIS

Voice phishing as a potential entry point

Why Vishing Is Effective

- Creates urgency and authority pressure
- Bypasses email security filters entirely
- Exploits trust in voice communication
- Targets help desk and support staff
- Harder to verify caller identity in real time

Key Questions

- Which employees are most targeted?
- What habits make attacks succeed?
- How does ShinyHunters use impersonation?
- What hasn't been publicly confirmed?

Note: The exact initial access path in the Canvas incident has not been publicly confirmed. This is a working hypothesis based on known threat patterns.

HOW ATTACKS LIKE THIS BEGIN

Small-Group Discussion: Likely Initial Access Methods

Phishing

Fraudulent emails targeting credentials or session tokens

Credential Theft

Stolen or reused passwords from prior breaches

Token Abuse

Hijacked authentication tokens or API keys

Misconfiguration

Exposed endpoints or overly permissive access settings

Social Engineering

Manipulating support staff through impersonation

Third-Party Access

Compromised vendor or integration accounts

Discuss: What attack chain do you think is most plausible?

Call-Back Verification

Verify identity through a separate, trusted channel before acting on requests

Phishing-Resistant MFA

Implement hardware keys or biometric authentication that can't be phished

Stricter Help-Desk ID Checks

Require multi-factor identity confirmation for all support requests

Reduced Standing Privileges

Apply least-privilege access and just-in-time elevation policies

Enhanced Logging & Monitoring

Detect anomalous access patterns and respond quickly to alerts

User Education

Train staff to recognize urgency, authority, and impersonation cues

KEY TAKEAWAY

Large incidents are often not caused by a single exploit.

They frequently involve trust, persuasion, and gaps in verification.