CAMPUSGUARD®

CAN YOU SPOT A DEEPFAKE SCAM?

Deepfake scams are changing how cybercriminals trick people into trusting what they see and hear. With AI capable of cloning voices, generating realistic videos, and impersonating trusted individuals, students, faculty, and staff can no longer rely on familiar faces or voices as proof of legitimacy.

This quick guide highlights the warning signs and simple steps everyone on campus can take to spot and stop AI-generated fraud before it causes harm.

What is a Deepfake?

AI-generated video, audio, or images designed to impersonate real people and trick you into trusting a fake message.

Common Campus Scenarios

- “IT Support” video call asking for your password
- Voicemail from a “department head” requesting urgent action
- Fake video announcement about account issues
- Social media message from a “student” asking for help

Warning Signs

- Lip movements don’t perfectly match speech
- Robotic, flat, or unnatural voice tone
- Odd lighting, blinking, or facial movements
- Urgent request that bypasses normal process
- Message doesn’t match known schedules or policies

What To Do

- Pause – don’t react emotionally
- Verify through official email or directory
- Report to IT/security immediately
- Never share passwords or MFA codes

Stop. Think. Verify.

Your awareness protects the entire campus.