2025

Cybersecurity

ANNUAL TRAINING

THE BREACH: AGENT UNDERCOVER

Case Briefing

Case lead: Agent Josh Coyle

Case Overview:

Agent Josh Coyle will take over the case from Agent Reyes, who has been critically injured. Agent Coyle will infiltrate the scam center as a new employee. His relative inexperience as an agent makes him ideal for this covert role, as it lowers the risk of suspicion. Josh will be equipped with an earpiece and will be guided remotely by the Agency during his undercover operation.

Critical Information:

- The scam center is highly organized. They engage in cold calling, phishing, social engineering, and AI-assisted scams targeting individuals and corporations.
- The center has been operational for an extended period.
- The operation will rely on Agent Coyle maintaining the persona of a new, inexperienced employee with a background in tech support.

Objectives:

- Gain a better understanding of the scam center's operations.
- Identify key players and their roles.
- Gather evidence to dismantle the scam center's sophisticated web of criminal activity.
- Ensure safe extraction of any critical data or intel in order to initiate a bust.

Risks:

- The center is suspected to be behind the attack on Agent Reyes.
- The operation is considered high-risk due to the organized nature of the scam center and the potential for retaliation or violence.
- The criminals are tech-savvy and will detect any poorly concealed surveillance efforts. Josh will need to rely heavily on his training and guidance from the Agency.

Evidence Gathered:

- Reyes had identified several linked fraudulent websites, romance scams, and phishing schemes, but was still in the process of gathering concrete evidence at the time of her injury.

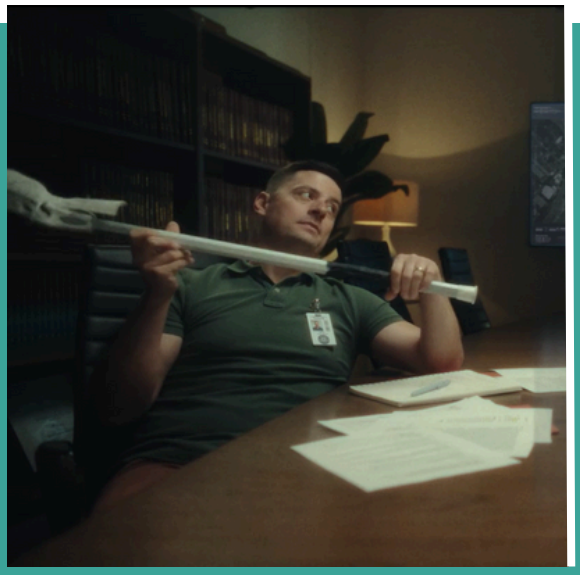
Contact Information:

For any queries or additional information, please contact:

Assistant Director Crutchfield

adcrutchfield@the agency.com

Phone Scams



Agent in Training- Day 1

“People need more training. They know phone scams exist, but scammers' tactics are constantly changing.”

-Agent Reyes

Phone Scams

Phone scams occur when a cybercriminal calls using threatening language or false promises to gather sensitive information or money. Scam calls have led to 29.8 billion dollars lost in just one year.

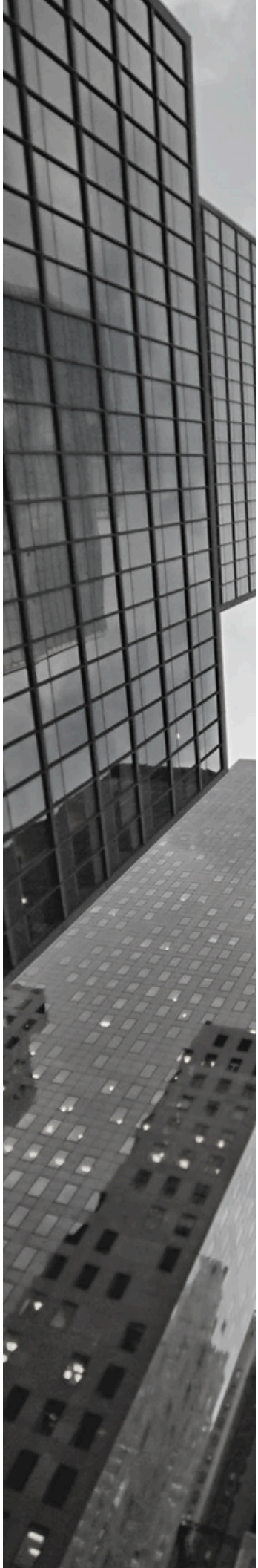
Best Practices:

- Don't divulge information to unsolicited callers.
- If you are skeptical about the call, hang up.
- Verify the legitimate number online or through your address book and call that one instead.

Artificial Intelligence in Phone Scams

With enough voice samples, artificial intelligence (AI) can generate audio to mimic anyone. This can come from a person’s voicemail, social media posts, or any other audio available to the public. Some scammers clone the voices of CEOs or high-level employees and even use the target's name and job title in their message.

Families and coworkers should have a secret word or phrase that only they know in order to verify urgent calls. It’s also best to call the person back on their normal phone number even if the voice on the other end claims they can't access it.



The Dark Web

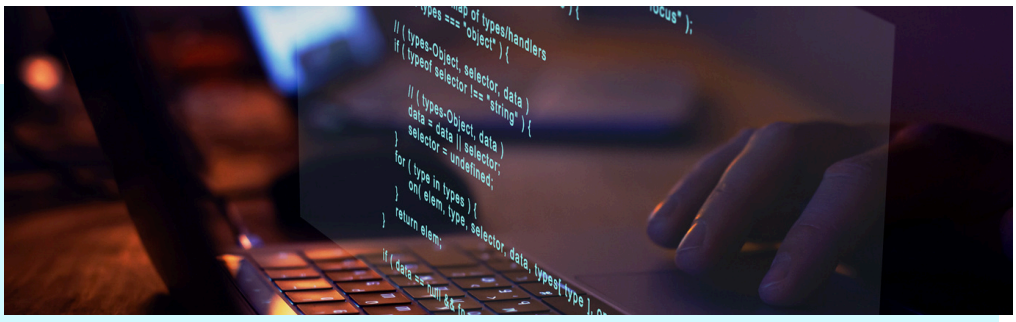
WHAT IS IT?

The dark web is a part of the World Wide Web and is only accessible through a specialized web browser called TOR. It is not traceable, so users remain anonymous. This means cybercriminals flock to the dark web to buy and sell information, malware, and users' data.

PII

PII stands for personally identifiable information. If PII such as someone's name, social security number, email address, or phone number ends up on the dark web, it can be purchased and used in ongoing scams.

Depending on what PII has been acquired and posted on the dark web, you should change any exposed passwords or usernames and monitor account activity closely.



Passwords

Password Managers

With one strong master password, password managers keep all your passwords secure. They also make it easier to follow best practices since many password managers generate strong passwords.

Multi-factor Authentication

Multi-factor authentication or MFA requires two or more forms of authentication to gain access to an account or system. It could require something you are, something you know, or something you have.

"On average, users reuse passwords across sixteen workplace accounts."

-Agent Reyes

Password Best Practices

Long

According to recent CISA guidelines, passwords should be at least 16 characters.

Unique

Each account should have its own unique password so that if one account suffers a breach, it doesn't impact others.

$4To

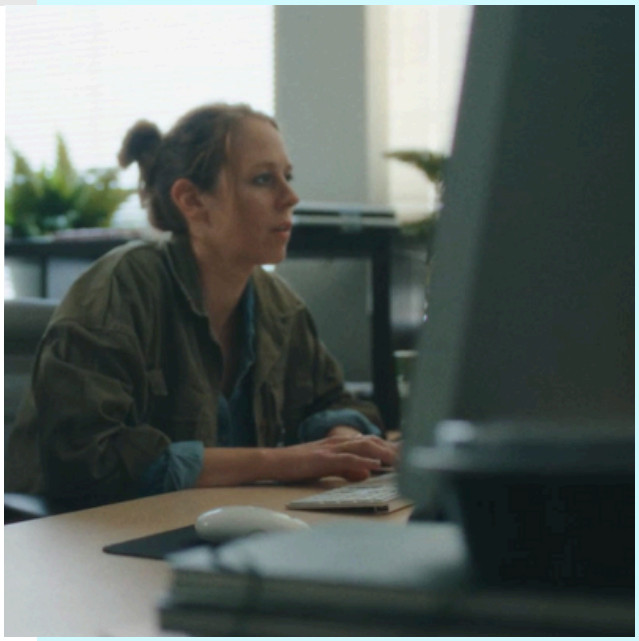
Mix of Characters

Avoid repeating the same character multiple times in a row or using one, simple to guess word.

Malicious Websites

Cali - “Web Designer”

“See how the URL is one letter off from the actual website? The letters are right next to each other on the keyboard so they might type the wrong URL. And the letters look similar so there is a chance the user will click the link by mistake.”



Pharming

Pharming uses malicious code to redirect users to fraudulent websites, even if they type in the real URL.

Typosquatting

A tactic where cybercriminals register domain names with common misspellings of trusted sites.

Spoofing

When cybercriminals impersonate someone or something to trick users into providing information.

Social Engineering

Social engineering involves psychologically manipulating people into giving away their information.

Spot Malicious Websites

Users should examine links and URLs before interacting with a website. Cybercriminals often try to mimic the URLs of legitimate websites to make users trust their site.

Websites and AI

Cybercriminals use AI when generating malicious websites to identify vulnerable systems, assist in cloning legitimate websites, and evade malware detection.

Phishing

Phishing Defined

Phishing refers to the practice of sending a message to a user with the malicious intent of trying to trick them into revealing sensitive information or installing malware.

AI in Phishing

Scammers are utilizing chatbots to write grammatically correct phishing emails, making scams difficult to spot off of spelling alone.

SLAM Method

Sender

Check if the email address or phone number is correct.

Links

Hover over, but don't click to see a link's true path.

Attachments

Analyze any expected or unsolicited documents.

Message

Be wary of threatening language or requests for sensitive information.

Vishing

Vishing or voice phishing refers to scams carried out through phone calls or voice messages.

Social Media

Cybercriminals can collect a user's information on social media and use it in their attacks. Social media accounts should be kept private.

Spear Phishing

A spear phishing attack occurs when a cybercriminal crafts a personalized message for their target. AI has made it easier than ever for cybercriminals to collect personal information and create convincing messages in the blink of an eye.

Insider Threats

Unintentional Insider Threats

An unintentional insider threat refers to an employee who harms the organization's security by accident, without any malicious intent.

Intentional Insider Threats

An intentional insider threat refers to when an employee deliberately tries to harm the organization through malicious activities like selling company data to a competitor.

Tailgating

A physical security breach where an unauthorized person follows an unsuspecting employee into a building that typically requires authorized access to enter.

Reporting

Report insider threats to a supervisor without engaging with the insider directly. To avoid becoming an unintentional insider threat, stay up to date on employee policies and take continuous cybersecurity training.

Malware & Ransomware

Malware

A malicious software designed to exploit systems. It can take various forms, including worms, ransomware, spyware, and more. Its purpose is to gain unauthorized access without users' knowledge. Disconnect any device infected with malware and report the incident immediately.

Ransomware

Ransomware is a type of malicious software designed to block access to a computer system or data until a ransom is paid. It typically encrypts the victim's files, and the attacker demands payment for the decryption key, often threatening to leak or destroy the data if the ransom isn't met. Ransomware can encrypt or steal sensitive data, with no guarantee of recovery or privacy even if the ransom is paid.

Best Practices

- **Updating Software**: Turn on automatic updates and update software immediately to patch any vulnerabilities.
- **Physical Security**: Keep filing cabinets, computers, and offices locked when not in use.
- **Backups**: Make sure all files are backed up in case of a breach or loss.

Repercussions

Ransomware attacks can shut down systems, halt operations and cause financial and reputational damage, especially in critical sectors like healthcare.