

Pasadena Citizens' Advisory Council

Plant Security II: Cybersecurity

May 27, 2025

The 316th meeting of the Pasadena Citizens' Advisory Council (PCAC) was held on Tuesday, May 27, 2025, at the Log Cabin in RYSS Stem Academy, 1062 Fairmont Parkway. Former FBI cybersecurity analyst James Morrison, Senior Director of Security Programs for Intelisys, discussed how cybercrime affects the community. Morrison opened his presentation by explaining that the trend in cybercrime has shifted from targeting corporations and governments to targeting average Americans because people in other countries think "all Americans are rich." Morrison shared some fascinating yet sobering stories of how cybercriminals catch their victims unaware, but he also offered some tips on how to safeguard personal information. Morrison's presentation included the following points:

Sobering insights:

- Federal law enforcement won't bother investigating "smaller scams" (\$5,000).
- Since many scams in the United States originate in different countries, local law enforcement has no jurisdiction.
- Most cybersecurity breaches begin with user actions—clicking links, sharing info, or poor password practices.
- Cyberattacks are shifting from email to phone calls and text messages.
- The dark web hosts a marketplace for stolen data, ransomware services, and even human trafficking.
- Caller ID is unreliable — numbers can be spoofed to look legitimate (e.g., sheriff's office, banks).
- Even known email addresses (like a relative's) can be hacked or impersonated.
- North Korean operatives pose as U.S.-based job applicants using AI to assist the scam.
- Use AI-driven deepfake video interviews to fool HR departments.

Strategies to defend against cyberattacks

- Tools like dark web monitoring (e.g., through LifeLock) can alert individuals to compromised information.
- Be skeptical of unsolicited contact, offers, or too-good-to-be-true deals.
- Use strong, unique passwords and consider cybersecurity tools that offer monitoring and alerts.
- If someone you don't know calls and asks you to repeat specific words or phrases — hang up.
- Never click unknown links or run files from unknown sources.
- You can take pictures from the lock screen — don't unlock your phone for someone to take a photo.
- Create better passwords:
 - Use a book. Open to a random page and choose 3 to 4 words.
 - Add special characters, capitalize letters, and substitute numbers for letters.
 - Write down the page number as a memory aid—not the actual password.
 - Aim for at least 20 characters; **length matters**.