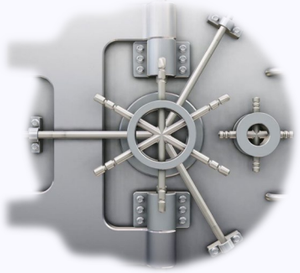
Cybercrime Challenges for Law Enforcement, the Public, and Our Profession

by Walter Houser
Volunteer with the Financial Crimes Section
Montgomery County Police Department



"You know, you can do this just as easily online."

Actually, it is easier.

Cybercrime Challenges for Law Enforcement

1 International Jurisdiction

Cybercrimes often originate outside U.S. borders, hindering investigations and prosecutions.

2 Resource Constraints

Local police lack trained cybersecurity personnel and resources to tackle complex digital crimes.

3 Evidentiary Hurdles

Digital crimes leave little physical evidence, making case building challenging.

4 Legal Ambiguities

Scammers exploit legal gray areas, leading to dismissed complaints and unresolved cases.

Barriers to Public Awareness

Overwhelming Information

The online world is confusing and overwhelming, making it difficult to know what to trust or how to stay safe.

Limited Knowledge

Many people lack the knowledge and skills to protect themselves online. Most only seek cybersecurity information after victimization.

Sense of Helplessness

Many people feel they have little control over their online security, leaving them vulnerable to cyber threats.

Barriers to Public Awareness

1 I’m Not a Target

Most people are unaware of how criminals can exploit anyone.

2 Surely It’s Secure?

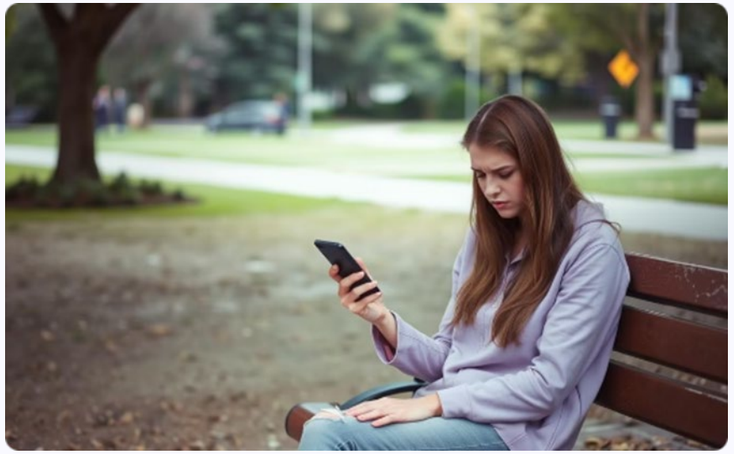
The public assumes hardware and software is safe because the vendors know so much more than we do.

3 Limited Resources

Few organized efforts exist to update the public on threats and vulnerabilities in a manner that suits the audience.

4 Shame and Embarrassment

Victims are often embarrassed and shamed, which deters them from reporting cybercrimes. Victim shaming is common.



Bridging the Cybersecurity Knowledge Gap

For Cyber Pros

Conduct community training sessions, workshops, and webinars.

Offer technical support and mentorship to help bridge the expertise gap.

Break down complex topics into clear, relatable messages.

For Law Enforcement

Equip officers with skills to investigate cybercrimes and manage digital evidence.

Build relationships with cybersecurity experts and companies.

Work alongside cybersecurity professionals to run public awareness campaigns.

Empowering the Public

Multi-Channel Communication

Utilize social media, community centers, schools, and public forums to spread awareness.

Local Partnerships

Collaborate with local leaders and influencers to amplify cybersecurity messages.

Encourage Reporting

Motivate the public to report suspicious activity and scams promptly.

Mentorship Programs

Guide students to address the growing cybersecurity skills gap in the workforce.

Future Cybersecurity Strategies and Solutions

Enforce standards for products and practices.

Build trust with the public by demonstrating efforts to protect them.

Foster collaboration between technologists, companies, law enforcement, and educators to strengthen cybersecurity efforts.

Continuously evolve strategies as threats evolve.

Translate complex concepts into actionable advice and keep both professionals and the public updated on emerging threats.

Better regulation and enforcement of cryptocurrency transactions.

Questions