Connected devices are essential to our professional and personal lives, and criminals have gravitated to these platforms as well. Many common crimes—like theft, fraud, harassment, and abuse—are now carried out online, using new technologies and tactics. Others, like cyber intrusions and attacks on critical infrastructure, have emerged as our dependence on connected systems revealed new vulnerabilities.

Successfully mitigating these threats relies on a combination of information sharing, prevention efforts, and enforcement work. Government agencies, law enforcement, the private sector, and individuals all have a role to play.

National Cybersecurity Awareness Month (https://staysafeonline.org/ncsam/) was created in 2004 by the Department of Homeland Security and the National Cyber Security Alliance to provide a reminder that each of us has the power to make the Internet safer and more secure.

“While the speed at which technology and information move can expose us to new risks online, it also enables a level of sharing and cooperation that can make us more resilient to cyber threats,” says FBI Cyber Division Assistant Director Matt Gorham. “National Cybersecurity Awareness Month isn’t just about understanding the risks, but also emphasizing our collective power to combat them.”

The FBI coordinates closely with the private sector as well as with state, local, and international partners to understand and anticipate cyber threats and pursue cyber criminals with every available resource.

Recently, the FBI’s work has resulted in the conviction of a cyber criminal who tried to access university databases to commit fraud and identity theft (https://www.fbi.gov/contact-us/field-offices/atlanta/news/press-releases/jury-convicts-cybercriminal-for-hacking-universities), charges against a North Korean regime-backed programmer (https://www.fbi.gov/news/pressrel/press-releases/north-korean-regime-backed-programmer-charged-with-conspiracy-to-conduct-multiple-cyber-attacks-and-intrusions), and 74 arrests in the United States and overseas of members of a transnational criminal network participating in business email compromise schemes. (https://www.fbi.gov/news/pressrel/press-releases/74-arrested-in-coordinated-international-enforcement-operation-targeting-hundreds-of-individuals-in-business-e-mail-compromise-schemes)

“National Cybersecurity Awareness Month isn’t just about understanding the risks, but also emphasizing our collective power to combat them.”

Matt Gorham, assistant director, FBI Cyber Division

“Realistically, we know we can’t prevent every attack, or punish every hacker,” FBI Director Christopher Wray told the Boston Conference on Cyber Security earlier this year. “But we can build on our capabilities. We can strengthen our partnerships and our defenses. We can get better at exchanging information to identify the telltale signs that may help us link cyber criminals to their crimes. And we can impose a variety of costs on criminals who think they can hide in the shadows of cyber space. We can do these things—and we are.”