Executive Viewpoint
A conversation with TONYA UGORETZ

TONYA UGORETZ
Deputy Assistant Director for the Cyber Readiness, Outreach and Intelligence Branch, FBI

An FBI cyber leader discusses how the bureau helps government and industry protect themselves from cyberthreats

What role does the FBI play in addressing cyberthreats?

The FBI has a long history of adapting to threats, starting with its creation over a hundred years ago to address interstate crime when automobiles made it easier for criminals to move across state lines. Since then, we've adapted our domestic field-centric model and our global presence to bring down dangerous criminal enterprises, foil terrorist plots and disrupt rings of foreign spies. When it comes to cyber intrusions, we apply that history of innovation and investigative expertise to meet the current threat.

We see the FBI as a linchpin in combating cyberthreats because they challenge the U.S. government's traditional approach of looking at threats as either foreign or domestic, or either criminal or national security. Cyberthreats involve both criminals and state actors typically operating from overseas and both using and compromising U.S. networks to target U.S. victims.

The FBI is in a unique position because we have an optic into parts of this entire threat ecosystem, combining information we glean from commercial threat intelligence, our long-standing relationships with industry, our incident response and investigations, our unique domestic intelligence authorities and foreign liaison, and our analysis as part of the Intelligence Community. We share that information and insight to improve network defense, to inform offensive operations and to help attribute malicious cyber activity to the responsible actors, which gives the U.S. government options to deter and respond.

What has the FBI observed regarding the pandemic's impact on the cyberthreat landscape?

Both cyber criminals and state actors have been active during the pandemic, for different reasons. An increase in telework, virtual education and government relief programs and the urgent demand for research and development have all created or exacerbated vulnerabilities.

There's a long history of criminals taking advantage of natural disasters and other crises for personal gain, and unfortunately the COVID-19 pandemic

> **The FBI has worked to actively disrupt cyber criminals** who are attempting to profit from the pandemic.

> **An increase in telework, virtual education and government relief programs** and the urgent demand for research and development have all created or exacerbated vulnerabilities.

has been no exception. To perpetrate scams, enterprising criminals are taking advantage of the high public demand for information about COVID and the rapid shift for many of us of our entire lives online. Numerous cybersecurity companies have remarked on this, and for the FBI, one key measure is the complaints we see coming in to our Internet Crime Complaint Center (IC3).

The IC3 has already received nearly as many complaints halfway through 2020 as it did for all of 2019, and thousands of those are COVID-related scams, such as offering fake vaccines, cures and protective equipment; trying to steal your information or money by promising information about stimulus checks; or using COVID-themed emails to deliver malware.

Meanwhile, state actors are using cyber intrusions to satisfy their own need for information — for example, targeting COVID-19-related research to accelerate their own R&D and clinical trials or to gain insight into how other countries are responding. The potential theft of this information jeopardizes the delivery of secure, effective and efficient treatment options. For example, we have been investigating the targeting and compromise of U.S. organizations conducting COVID-19-related research by cyber actors and nontraditional collectors tied to the People's Republic of China.

On May 13, the FBI and the Department of Homeland Security released a public service announcement to warn members of the health care, pharmaceutical and research sectors working on COVID-19 response to be aware that they are the prime targets of this activity and to take the necessary steps to protect their systems.

How is the FBI helping public and private organizations adapt to pandemic-related threats?

We realize that with the speed and complexity of cyberthreats, we need to immediately share information we learn that can help public and private organizations protect themselves even as we pursue longer-term efforts to attribute malicious activity and hold those responsible accountable.

The FBI has been sharing information about specific threats and trends we've observed associated with COVID-19 since the start of the pandemic. Recently, we published a Private Industry Notification about the targeting of telework employees through phishing emails masquerading as legitimate meeting invites or notices of termination. We've also noted tactics used by cyber criminals for K-12 educators to be aware of. We will continue to push out information as we see trends in targeted industries or adversary tactics to ensure organizations and individuals are protected.

In addition to sharing information broadly, we have been coordinating closely with DHS and the Department of Health and Human Services on our engagement with the private sector, focusing on those who are at increased risk of targeting due to their involvement with the national COVID-19 response. The FBI has worked to actively disrupt cyber criminals who are attempting to profit from the pandemic. Together with our partners, we have sent hundreds of referrals to private-sector companies managing or hosting domains suspected in fraudulent activity. Many of those companies, in turn, have taken down the domains after concluding that they violated their abuse policies and terms of service, without requiring legal process.

What are some best practices for ensuring individuals and companies are protected from cyberthreats?

The FBI urges the public to remain vigilant. While criminals try to take advantage of this vulnerable moment, we can protect ourselves by not letting our guard down.

It is still the case that some of the most exploited vulnerabilities, even by sophisticated state actors, are ones that have long had patches available. To help address this, in May, the FBI and DHS issued an alert identifying the top 10 most routinely exploited vulnerabilities. What we've observed is that our adversaries are still going after low-hanging fruit — vulnerabilities that have been out for a while and thus require fewer resources to exploit.

This highlights that the most important thing is still to exercise basic cyber hygiene: patch systems as soon as practicable, educate your workforce about common adversary tactics such as phishing and social engineering, and implement programs to ensure software is up-to-date. These simple steps will lower your risk by reducing your attack surface and at the very least may make the adversary work harder and think twice before making you a target.

Visit IC3.gov for the latest public alerts and more tips to keep your agency safe during the pandemic and beyond.