

US > CRIME & PUBLIC SAFETY

FBI Issues Joint Warning on Hackers Targeting Email Accounts

The FBI and several other U.S. agencies issued a joint cybersecurity advisory.

 634  313  Saved



An FBI agent walks toward a crime scene in Gilroy, Calif., on July 29, 2019. (Mario Tama/Getty Images)



By [Jack Phillips](#)

   Print

5/6/2024 Updated: 5/7/2024

The FBI and several U.S. agencies issued a joint cybersecurity advisory that warned of state-backed hacks using emails in a way that makes them appear to be from legitimate and trusted organizations.

In the joint [statement](#), the FBI, U.S. Department of State, and National Security Agency (NSA) said that alleged North Korean-backed hackers linked to the communist country's military intelligence agency, known as Kimsuky, have been using email authentication bypass to impersonate academics, journalists, and researchers.

They are now attempting to “provide stolen data and valuable geopolitical insight to the North Korean regime by compromising policy analysts and other experts,” the bulletin said.

“Successful compromises further enable Kimsuky actors to craft more credible and effective spear-phishing emails, which can then be leveraged against more sensitive, higher-value targets,” it said.

The hacking group wants to keep “consistent access to current intelligence about the United States, South Korea, and other countries of interest to impede any perceived political, military, or economic threat to the regime's security and stability,” the bulletin stated.

“In addition to convincing email messages, Kimsuky cyber actors have been observed creating fake usernames and using legitimate domain names to impersonate individuals from trusted organizations, including think tanks and higher education institutions, to gain trust and build rapport with email recipients,” it read.

But those emails don't come from the organization's “actual domain email exchange, but rather from the actor-controlled email address and domain,” the statement added.

“Even if a skeptical recipient wanted to verify whether the sender was legitimate, the recipient email response would be sent back to a spoofed email address at the trusted domain,” it read.

The FBI, State Department, and NSA notice urges all email users to move to prevent such hackers from going through. It said that people should update their email accounts' DMARC—which stands for “domain-based message authentication, reporting and conformance”—policies. However, users of email services such as Gmail and Yahoo should not be concerned as both companies confirmed they would automatically implement more stringent DMARC policies.

The Big Picture Connected to FBI Source Arrest | Truth Over News

Last month, FBI Director Christopher Wray issued warnings about state-backed hackers in China, Russia, Iran, and North Korea as he called for more congressional funding for his agency.

“We need funding to counter cyber threats—certainly those from China, but also from a crowded field of sophisticated criminals and other hostile nation-states like Russia, Iran, and North Korea,” he stated, although he noted that the Chinese Communist Party (CCP) appears to be of most concern to U.S. officials.

“[The CCP is] sparing no expense in its quest to hack, lie, cheat, and steal its way to the top as a global superpower and to undermine our democracy and our economic success,” he said, according to an FBI transcript of his remarks at a House committee.

The joint notice comes as the FBI recently found that various scammers stole more than \$3.4 billion from older Americans last year, according to an FBI report.

Losses from scams reported by Americans over the age of 60 last year were up 11 percent over the year before, according to the FBI’s report. Investigators are warning of a rise in brazen schemes to drain bank accounts that involve sending couriers in person to collect cash or gold from victims.

“It can be a devastating impact to older Americans who lack the ability to go out and make money,” Deputy Assistant Director James Barnacle of the FBI’s Criminal Investigative Division said in a statement. “People lose all their money. Some people become destitute.”

The FBI received more than 100,000 complaints by victims of scams older than 60 last year, with nearly 6,000 people losing more than \$100,000. It follows a sharp rise in reported losses by older Americans in the two years after the COVID-19 pandemic, when people were stuck at home, making it easier for scammers to reach them over the phone.

But the staggering total of losses by older Americans is likely an undercount. Only about half of the more than 880,000 complaints reported to the FBI’s Internet Crime Complaint Center last year included information on the age of the victim.

The Associated Press contributed to this report.

SHARE THIS ARTICLE



Jack Phillips
Author (Breaking News Reporter)

Jack Phillips is a breaking news reporter with 15 years experience who started as a local New York City reporter. Having joined The Epoch Times' news team in 2009, Jack was born and raised near Modesto in California's Central Valley. Follow him on X:

<https://twitter.com/jackphillips5>



Author's Selected Articles

House GOP Sends Michael Cohen Criminal Referral to Justice Department

May 08, 2024



Trump Decries Inability to Respond to 'Lies And False Statements' Made in Trial

May 08, 2024



Jack Smith Has Few Options in Trump Case, Say Former Prosecutors

May 08, 2024



Secret Service 'Must Provide Protection' to Trump If He's Jailed: Spokesperson

May 08, 2024

