

USA

FBI: Surge in Internet Crime Cost Americans \$4.2 Billion

By Masood Farivar

March 17, 2021 08:13 PM



The FBI says it received a record number of complaints from the public last year about cybercrimes, including scams related to the COVID-19 pandemic, costing Americans a staggering \$4.2 billion in losses.

The FBI's Internet Crime Complaint Center received 791,790 complaints in 2020, an increase of 69% over 2019 and the largest number since the center was created two decades ago, the bureau said in a report released Wednesday.

By comparison, the total reported losses were \$3.5 billion in 2019 and \$1.5 billion five years ago, according to the report.

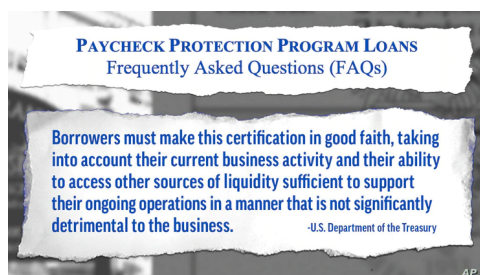
The type of online scam known as Business E-Email Compromise (BEC) remained the costliest category, the report said, resulting in losses of about \$1.8 billion. Once a fraudster gains access to a business's email account, he or she makes unauthorized fund transfers.

The COVID-19 outbreak gave scammers new opportunities to steal. The FBI internet crime center received more than 28,500 complaints related to people struggling to cope with the pandemic, the report said, without putting a dollar figure on the losses.

Most vulnerable are targeted

“These criminals used phishing, spoofing, extortion, and various types of Internet-enabled fraud to target the most vulnerable in our society – medical workers searching for personal protective equipment, families looking for information about stimulus checks to help pay bills, and many others,” the report said.

The center received thousands of complaints related to COVID-linked unemployment benefit and small business loan programs Congress created last year.



The congressionally funded Paycheck Protection Program has proven a magnet for fraudsters. Congress created the program last March with an initial authorization of up to \$349 billion in forgivable loans to small businesses that keep workers on their payrolls. The Justice Department has charged numerous individuals with defrauding the program by setting up shell companies and other schemes.

In the latest case, tech executive Mukund Mohan pleaded guilty on Monday of wire fraud and money laundering in connection with his scheme to obtain over \$5.5 million in PPP loans and launder the proceeds.

The top three crimes reported to the FBI’s internet crime center last year were phishing or password theft scams, nonpayment/nondelivery scams and extortion, the report said.

In a nonpayment scheme, goods and services are shipped but payment is never made. A nondelivery scheme involves receiving payment without supplying

goods and services.

Identity theft utilized

In several states, fraudsters filed illegal unemployment benefit claims using stolen identities, according to the report.

“Many victims of this identity theft scheme did not know they had been targeted until they attempted to file their own legitimate claim for unemployment insurance benefits,” the report said.

In recent months, a slew of new scams related to COVID vaccines has emerged: schemes asking people to pay out of pocket to receive a vaccine, put their names on a vaccine waiting list or obtain early access.

“Fraudulent advertisements for vaccines popped up on social media platforms, or came via email, telephone calls, online, or from unsolicited/unknown sources,” the report said.

The FBI’s Internet Crime Complaint Center was set up in 2000 as part of the bureau’s effort to combat cybercrime. It has received 5.8 million complaints, some of which have been referred to law enforcement agencies for investigation.

RELATED STORIES

COVID-19 Pandemic

UN Warns Cybercrime on Rise During Pandemic

Crisis has produced 600% increase in malicious emails



By **Associated Press**
Sat, 05/23/2020 - 08:21 PM

COVID-19 Pandemic

EU Commission Warns of Increased Cybercrime During Coronavirus Crisis

Authorities say more people working from home increases susceptibility to on-line scams



By **VOA News**

Tue, 03/24/2020 - 03:28 PM



By

Masood Farivar

