

TRENDS

The 2020 Internet Crime Report highlights the IC3's efforts over the past year, specifically focusing on their efforts regarding Business Email Compromise (BEC) and Email Account Compromise (EAC) scams, Ransomware, and Tech Support Fraud.

Business Email Compromise :

In 2020, the IC3 received 19,369 Business Email Compromise (BEC)/ Email Account Compromise (EAC) complaints with adjusted losses of over \$1.8 billion. BEC/EAC is a sophisticated scam targeting both businesses and individuals performing transfers of funds. The scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

Ransomware:

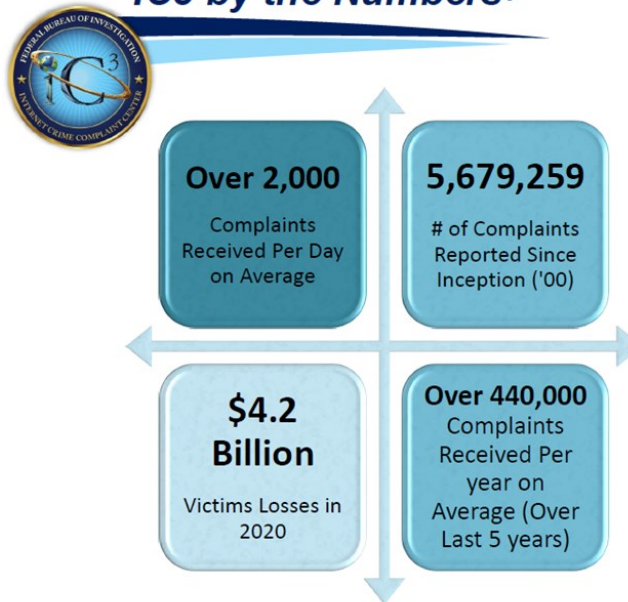
In 2020, the IC3 received 2,474 complaints identified as ransomware with adjusted losses of over \$29.1 million. Ransomware is a type of malicious software, or malware, that encrypts data on a computer making it unusable. A malicious cyber criminal holds the data hostage until the ransom is paid. If the ransom is not paid, the victim's data remains unavailable. Cyber criminals may also pressure victims to pay the ransom by threatening to destroy the victim's data or to release it to the public.

Tech Support Fraud:

Tech Support Fraud continues to be a growing problem. This scheme involves a criminal claiming to provide customer, security, or technical support or service to defraud unwitting individuals. In 2020, the IC3 received 15,421 complaints related to Tech Support Fraud from victims in 60 countries and the losses amounted to over \$146 million.

2020 STATISTICS

IC3 by the Numbers[®]



IC3 Complaint Statistics

Last Five Years

2,211,396 TOTAL COMPLAINTS



\$13.3 Billion TOTAL LOSSES*

(Rounded to the nearest million)



www.ic3.gov

AN INVESTIGATIVE LOOK INTO THE IC3

Mission of the IC3:

The mission of the Internet Crime Complaint Center (IC3) is to provide the public with a reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation concerning suspected Internet-facilitated criminal activity and to develop effective alliances with industry partners. Information is processed for investigative and intelligence purposes for law enforcement and public awareness.

Elder Fraud:

The Elder Abuse Prevention and Prosecution Act was signed into law in October 2017 to prevent elder abuse and exploitation and improve the justice system's response to victims in elder abuse and exploitation cases. As a response to the increasing prevalence of fraud against the elderly, the Department of Justice and the FBI partnered to create the Elder Justice Initiative. Elder Fraud is defined as a financial fraud scheme which targets or disproportionately affects people over the age of 60.

The FBI, including IC3, has worked tirelessly to educate this population on how to take steps to protect themselves from being victimized. In 2020, the IC3 received 105,301 complaints from victims over the age of 60 with total losses in excess of \$966 million. Since, age is not a required reporting field, these statistics only reflect complaints in which the victim voluntarily provided their age range as "OVER 60." Victims over the age of 60 are targeted by perpetrators because they are believed to have significant financial resources.

Internet Crime and the IC3:

As technology evolves, so do the many methods used to exploit technology for criminal purposes. Nearly all crime that once was committed in person, by mail, or over the telephone can be committed over the Internet. The criminal element is empowered by the perceived anonymity of the Internet and the ease of access to potential victims. Criminals use social engineering to prey on their victims' sympathy, generosity, or vulnerability. The IC3 was designed to help address all types of Internet crime through its complaint system.

IC3 Complaints:

The complaints submitted to the IC3 cover an array of Internet crime including theft of intellectual property rights, computer intrusion, economic espionage, online extortion, and international money laundering. Numerous fraud schemes such as identity theft, phishing, spam, reshipping, auction fraud, payment fraud, counterfeit goods, romance scams, and non-delivery of goods are reported to the IC3.



Searching the IC3 Database:

A remote search capability of the IC3 database is available to all sworn law enforcement through the FBI's Law Enforcement Enterprise Portal (LEEP). Users can connect directly to the IC3 Complaint Search after authenticating through LEEP from the user's Identity Provider (IDP) or through the user's Law Enforcement Online membership at www.cjis.gov. Users may also contact the IC3 for analytical assistance.

IC3 users have the ability to gather complaint statistics by city, state, county, or country and filter by crime type and victim age. Users can also run overall crime type reports and sort by city, state, and country. The report results can be returned as a PDF or exported to Excel. This search capability allows users to better understand the scope of cyber crime in their area of jurisdiction and enhance case development.

Public Service Announcements:

The IC3 reviews and analyzes data submitted through its website, and produces intelligence products to highlight emerging threats and new trends. Public service announcements (PSAs) and other publications outlining specific scams are posted to the www.ic3.gov website.