TRENDS

The 2019 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 and Ransomware.

Business Email Compromise :

In 2019, the IC3 received 23,775 Business Email Compromise (BEC) / Email Account Compromise (EAC) complaints with adjusted losses of over $1.7 billion. BEC/EAC is a sophisticated scam targeting both businesses and individuals performing a transfer of funds. The scam is frequently carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

Ransomware:

Ransomware is a form of malware targeting both human and technical weaknesses in an effort to make critical data and/or systems inaccessible. Ransomware is delivered through various vectors, including Remote Desktop Protocol, which allows computers to connect to each other across a network, and phishing. In 2019, the IC3 received 2,047 complaints Identified as ransomware with adjusted losses of over $8.9 million.

2019 STATISTICS

$3,501,693,146

- Losses Reported

467,361

- Complaints Received

141,590

- Complaints Received that Reported Losses

$24,731

- Average Loss for Complaints that Reported Losses

$7,492

- Average Loss for all Complaints

IC3 Complaint Statistics

Last Five Years

1,707,618 TOTAL COMPLAINTS

2015	2016	2017	2018	2019
288,012	298,728	301,580	351,937	467,361

2015	2016	2017	2018	2019
$1.1 Billion*	$1.5 Billion*	$1.4 Billion*	$2.7 Billion*	$3.5 Billion*

$10.2 Billion TOTAL LOSSES*

(Rounded to the nearest million)

FEDERAL BUREAU OF INVESTIGATION
IC3
INTERNET CRIME COMPLAINT CENTER

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. In June 2019, the Transnational Elder Fraud Strike Force was formed to investigate and prosecute entities associated with foreign-based fraud schemes targeting Americans, especially the elderly. The Strike Force combines the expertise and resources of the Department of Justice, FBI, U.S. Postal Inspection Service, and other organizations. The FBI, including IC3, has worked tirelessly to support this initiative and educate the public on how to take steps to protect themselves from being victimized. In 2019, the IC3 released PSAs to educate the public about Romance Fraud, common Elder Fraud schemes, and money mule activity. The FBI has held hundreds of outreach events to educate the public about Elder Fraud.

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.