New FBI Internet Crime Report

Richard P. Kusserow | April 15, 2021

Key Points:

- **The report includes COVID-19 scam and state-level statistics.**
- **Tips for preventing attacks are included below.**

The Internet Crime Complaint Center (IC3) of the Federal Bureau of Investigation (FBI) issued its annual report on cybercrimes reported by the general public. The *2020 Internet Crime Report* notes that IC3 received nearly 800,000 complaints of suspected internet crime last year, which represents an increase of more than 300,000 complaints from the prior year. Reported losses from the complaints exceed $4.2 billion.

Since 2016, IC3 has received more than 2.2 million complaints that involve more than $13 billion in losses. A press release associated with the report notes that the top three crimes reported in 2020 were phishing scams, non-payment/non-delivery scams, and extortion. Business email compromise scams, romance and confidence schemes, and investment fraud caused the most victims the most financial loss. There were also more than 28,500 complaints related to scams that exploited the COVID-19 pandemic and targeted both businesses and individuals. It is also noteworthy that IC3 received more than 100,000 complaints from victims over the age of 60, who experienced losses of about $1 billion.

Separately, IBM Security X-Force issued the *2021 X-Force Threat Intelligence Index*, which reports that the number of cyberattacks in various industries more than doubled in 2020, with ransomware accounting for nearly 28% of attacks in the health care sector. Of the 10 most-attacked industries, health care ranked tenth in 2019 but seventh in 2021. The rise in attacks was likely driven by the COVID-19 pandemic and ransomware attacks against hospitals. Health care also ranked third among industries subject to server-access attacks.

According to the cloud security company Bitglass, data compiled by the Department of Health and Human Services indicates that the number of health care breaches rose from 386 in 2019 to 599 in 2020, or an increase of 55.2%. More than 67 percent of the breaches were caused by hacking and information technology incidents. Collectively, more than 26.4 million individuals in the United States were affected by health care data breaches in 2020.

Tips for Guarding Against Cyber Attacks

1. Develop and implement cybersecurity policies.
2. Ensure that employees receive training on cyber security policies and principles.
3. Install, use, and regularly update antivirus and antispyware software on all computers.
4. Install spam filters and anti-malware software.
5. Deploy state-of-the-art firewalls for your network.
6. Develop a detection and response plan for cyber attacks.
7. Download and install software updates for systems and applications as they become available.
8. Make backup copies of important business data and information.
9. Control physical access to your computers and network components.
10. If there is a Wi-Fi network in the workplace, make sure it is secure and password-protected.
11. Require an individual user account for each employee.
12. Limit employee access to data and information and limit authority to install software.
13. Regularly change passwords.
14. Perform periodic vulnerability assessments.
15. Conduct routine penetration testing.