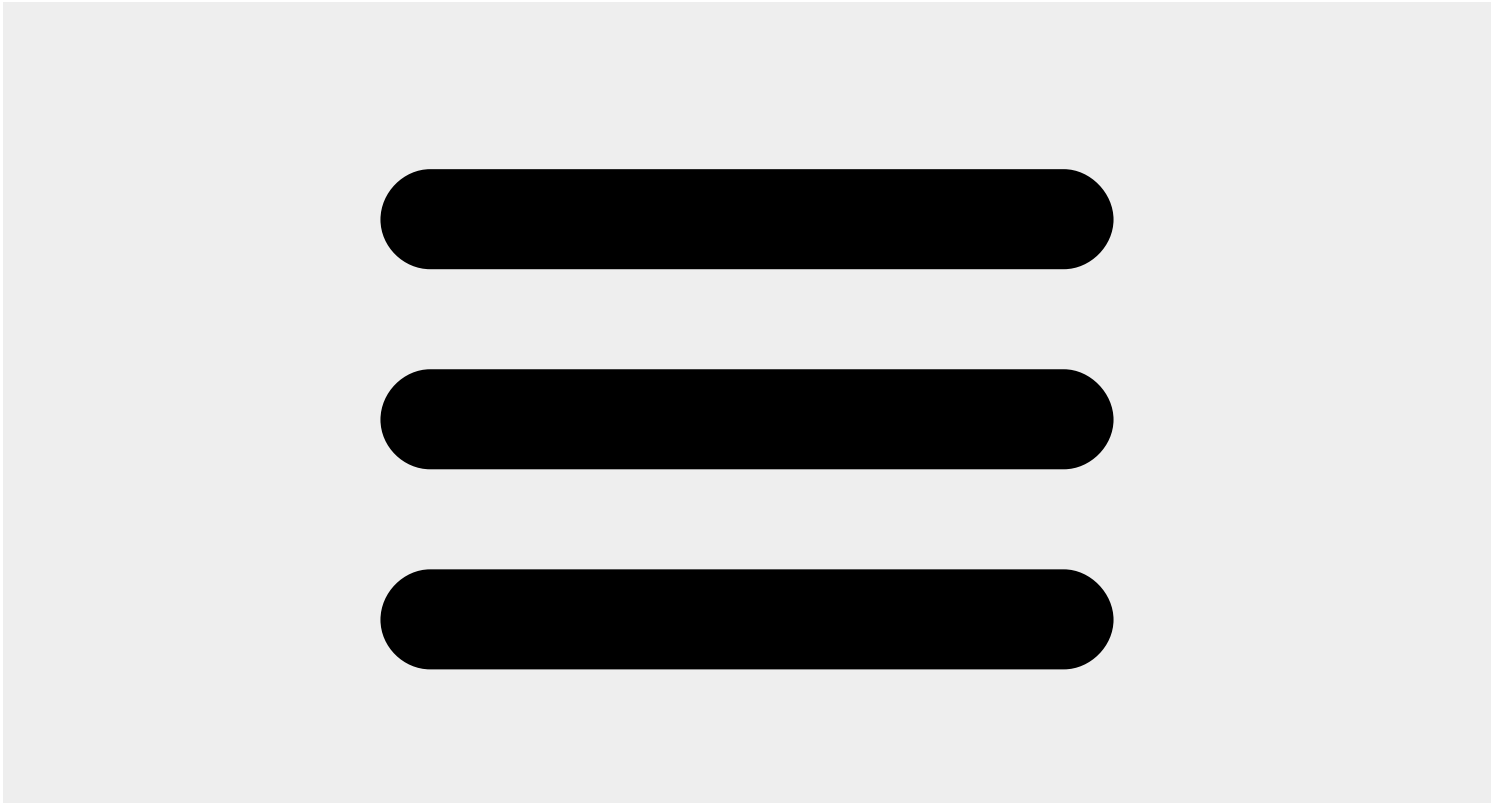
FBI 2020 INTERNET CRIME REPORT: WHAT ABOUT IT AND WHAT SHOULD WE DO?

Posted on May 18, 2021 by IACS Admin Team



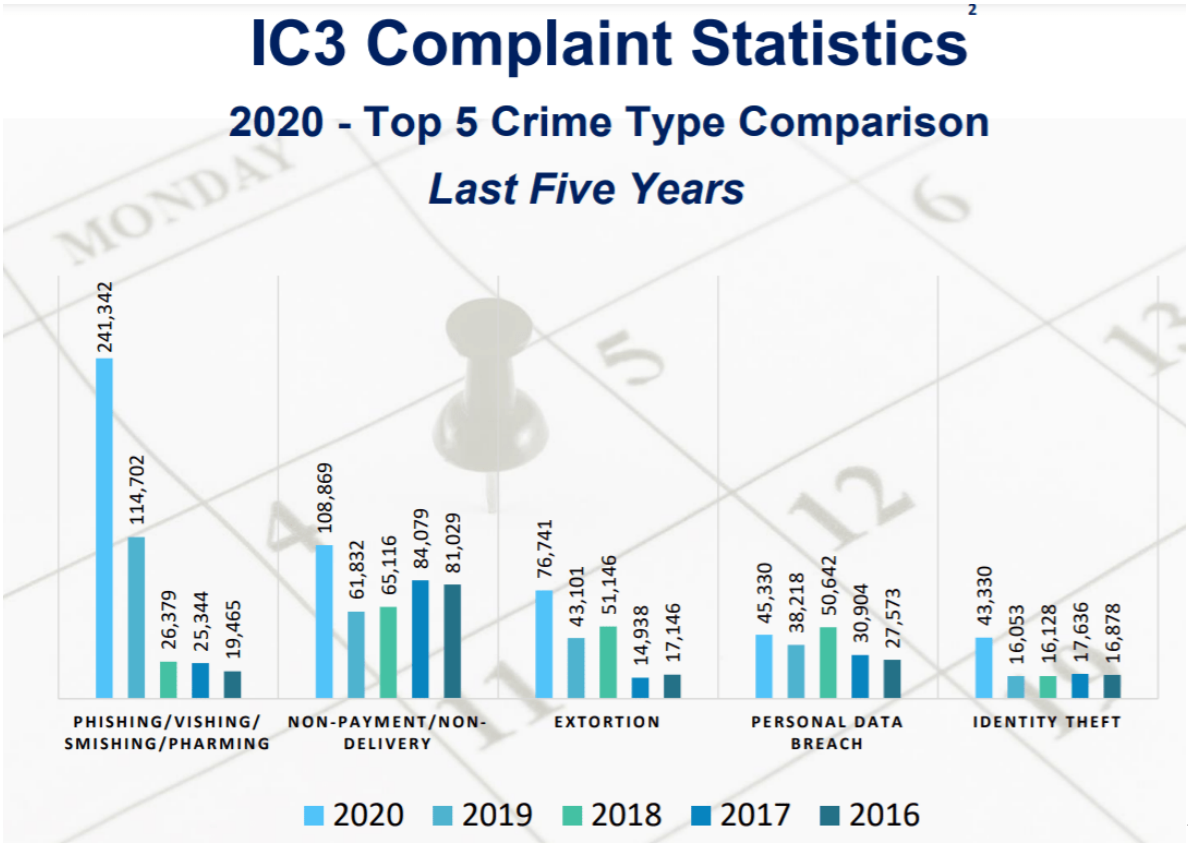
Category: Blog

Top Internet Crimes in 2020

The FBI's Internet Crime Complaint Center has released its annual Internet Crime Report on May 17, 2021. In this report, the center collected information from 791,790 complaints of suspected internet crime. Compared to the previous year in 2019, there is an increase of more than 300,000 complaints, a 69% increase in total complaints. The reported losses exceed $4.2 billion. It suggests that internet crime continues posting a threat to businesses and individuals in 2020. The top three crimes in 2020 were Phishing/Vishing/Smishing/Pharming scams (241,342 victims), non-payment/non-

delivery scams (108,869 victims), and extortion (76,741 victims).

> ***Phishing/Vishing/Smishing/Pharming*** *uses unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.* ***Non-payment*** *is the situation where goods and services are shipped, but payment is never rendered. In* ***non-delivery*** *situations, payment is sent, but goods and services are never received.* ***Extortion*** *is the unlawful extraction of money or property through intimidation or undue exercise of authority. It may include threats of physical harm, criminal prosecution, or public exposure.*



The five most prevalent types of crime based on victim reports filed with the FBI in recent years (Source: FBI)

Crimes Related to COVID-19

More significantly, this report includes the statistics relating to COVID-19 for the first time. Due to the COVID-19 pandemic, the scammers exploited the pandemic to conduct illicit internet crimes. In 2020, the center received more than 28,500 complaints related to COVID-19, with fraudsters targeting both businesses and individuals. Regarding

business, scammers targeted the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), which included provisions to help small businesses during the pandemic. Most IC3 complaints related to CARES Act fraud involved grant fraud, loan fraud, and phishing for Personally Identifiable Information (PII).

Concerning individual victims, government impersonators are one of the most prevalent schemes during the pandemic. Criminals are reaching out to people through social media, emails, or phone calls pretending to be from the government. The scammers attempt to gather personal information or illicit money through charades or threats. Additionally, vaccine-related scams have also emerged. Fraudulent advertisements for vaccines popped up on social media platforms or came via email, telephone calls, online, or from unsolicited/unknown sources.

What Should We Do?

To protect yourself, some safety tips are essential:

1. **Phone calls:** Be wary of answering phone calls from numbers you do not recognize.
2. **Emails:** Verify the sender of an email. Criminals will sometimes change just one letter in an email address to make it look like the one you know.
3. **Money transfer:** Never give out your personally identifiable information or send money or gift cards to anyone you don't know or trust.
4. **Information source:** Relying on trusted sources, like your own doctor, the Center for Disease Control, and your local health department for medical information and agencies like the Federal Trade Commission and Internal Revenue Service for financial and tax information.

Source: FBI IC3 Annual Report (2020): https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Citation suggestion: *Institute for Asian Crime and Security, IACS (2021): FBI 2020 Internet Crime Report: What About It And What Should We Do?. figshare. Online resource. https://doi.org/10.6084/m9.figshare.15127764.v1*