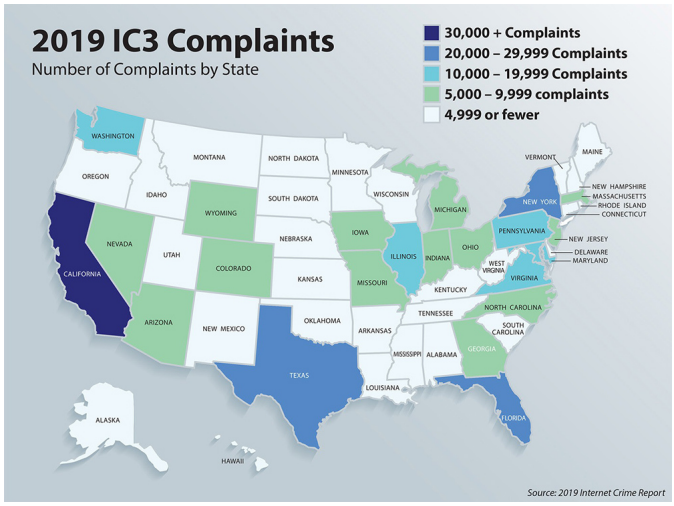

Watch out for smishing, pharming, fraud with your paycheck

Internet-enabled crimes and scams show no signs of letting up, according to data released by the FBI's Internet Crime Complaint Center (IC3) in its 2019 Internet Crime Report. The last calendar year saw both the highest number of complaints and the highest dollar losses reported since the center was established in May 2000.

New Mexico had 2,037 victims and $17,983,833 in losses in 2019.

In 2018, New Mexico had 2,127 victims for $8,617,772 in losses.

IC3 received 467,361 complaints in 2019—an average of nearly 1,300 every day—and recorded more than $3.5 billion in losses to individual and business victims. The most frequently reported complaints were phishing and similar ploys, non-payment/non-delivery scams, and extortion. The most financially costly complaints involved business email compromise, romance or confidence fraud, and spoofing, or mimicking the account of a person or vendor known to the victim to gather personal or financial information.

Donna Gregory, the chief of IC3, said that in 2019 the center didn't see an uptick in new types of fraud but rather saw criminals deploying new tactics and techniques to carry out existing scams.

"Criminals are getting so sophisticated," Gregory said. "It is getting harder and harder for victims to spot the red flags and tell real from fake."

While email is still a common entry point, frauds are also beginning on text messages—a crime called smishing—or even fake websites—a tactic called pharming.

"You may get a text message that appears to be your bank asking you to verify information on your account," said Gregory. "Or you may even search a service online and inadvertently end up on a fraudulent site that gathers your bank or credit card information."

Individuals need to be extremely skeptical and double check everything, Gregory emphasized. "In the same way your bank and online accounts have started to require two-factor authentication - apply that to your life," she said. "Verify requests in person or by phone, double check web and email addresses, and don't follow the links provided in any messages."

Shifts in Business Email Compromise

Business email compromise (BEC), or email account compromise, has been a major concern for years. In 2019, IC3 recorded 23,775 complaints about BEC, which resulted in more than $1.7 billion in losses.

These scams typically involve a criminal spoofing or mimicking a legitimate email address. For example, an individual will receive a message that appears to be from an executive within their company or a business with which an individual has a relationship. The email will request a payment, wire transfer, or gift card purchase that seems legitimate, but actually funnels money directly to a criminal.

In the last year, IC3 reported seeing an increase in the number of BEC complaints related to the diversion of payroll funds. “In this type of scheme, a company’s human resources or payroll department receives an email appearing to be from an employee requesting to update their direct deposit information for the current pay period,” the report said. The change instead routes an employee’s paycheck to a criminal.

The Importance of Reporting

“Information reported to the IC3 plays a vital role in the FBI’s ability to understand our cyber adversaries and their motives, which, in turn, helps us to impose risks and consequences on those who break our laws and threaten our national security,” Matt Gorham said. Gorham is the assistant director of the FBI’s Cyber Division. “It is through these efforts we hope to build a safer and more secure cyber landscape.” Gorham encourages everyone to use IC3 and reach out to their local field office to report malicious activity.

Rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good. The FBI’s Recovery Asset Team was created to streamline communication with financial institutions and FBI field offices and is continuing to build on its success. The team successfully recovered more than $300 million for victims in 2019.

Besides stressing vigilance on the part of every connected citizen, the IC3’s Donna Gregory also stressed the importance of victims providing as much information as possible when they come to IC3. Victims should include every piece of information they have - any email addresses, account information they were given, phone numbers scammers called from, and other details. The more information IC3 can gather, the more it helps combat the criminals.

In 2019, the Recovery Asset Team was paired with the Money Mule Team under the IC3’s Recovery and Investigative Development Team. This effort brings together law enforcement and financial institutions to use the data provided in IC3 complaints to gain a better view of the networks and methods of cyber fraudsters and identify the perpetrators.

The new effort allowed IC3 to aggregate more than three years of reports to help build a case against an active group of criminals who were responsible for damaging crimes that ranged from cryptocurrency theft to online extortion. The ensuing investigation by the FBI’s San

Francisco Field Office resulted in the arrest of three people.

For more information or to report a crime: ic3.gov.

Staff Reports