BUILT FOR
BETTER BUSINESS

Keeping your information safe

INTERNET FRAUD: TRENDS & INSIGHTS

Technology has become a staple among consumers, with 90% of us owning a smart phone or a laptop and the majority using online shopping or online banking according to a recent Experian study. While convenient, the widespread use of technology has opened up the flood gates for fraud. When technology is used to defraud consumers and take advantage of them in one way or another, this is known as Internet Crimes that take place via the Internet steal millions of dollars each year from victims and continue to plague the economic environment. In the most recent reporting year, the FBI's Internet Crime Complaint Center received more than 300,000 complaints with losses exceeding $1.4 Billion.

Source: FBI Internet Crimes Complaint Center (2017)

The prevalence of Internet fraud creates a need to recognize what constitutes cyber-crime, and what steps can be taken to prevent it.

Common Types of Fraud

1. **Non-Payment / Non-Delivery:**
   In non-payment situations, goods and services are shipped, but payment is never rendered. In non-delivery situations, payment is sent, but goods and services are never received.
2. **Misrepresentation:**
   Merchandise or services purchased or contracted by individuals online for which the purchasers provided payment, but what is received is of a measurably lesser quality or quantity than was described by the seller.
3. **Business Email Compromise (BEC):**
   BEC is a scam targeting businesses working with foreign suppliers and/or businesses regularly performing wire transfer payments. EAC is a similar scam that targets individuals. These sophisticated scams are carried out by fraudsters compromising email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfer of funds.
4. **Tech Support Fraud:**
   Attempts to gain access to a victim's electronic device by falsely claiming to offer tech support, usually for a well-known company is becoming more common. The fraudsters asks for remote access to the victim's device to clean-up viruses or malware, or to facilitate a refund for prior support services.
5. **Phishing / Vishing / Smishing / Pharming:**
   Unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.
6. **Identity Theft / Account Takeover:**
   Identify theft involves a perpetrator stealing another person's personal identifying information, such as name or Social Security number, without permission to commit fraud. Account Takeover is when a perpetrator obtains account information to perpetrate fraud on existing accounts.
7. **Romance Fraud:**
   A perpetrator deceives a victim by building a trust relationship, and then uses that trust to defraud victims.
8. **Charity Fraud:**
   Perpetrators set up false charities, usually following natural disasters, and profit from individuals who believe they are making donations to legitimate charitable organizations.
9. **Social Media Fraud:**
   A complaint alleging the use of social networking or social media (Facebook, Twitter, Instagram, chat rooms, etc.) as a vector for fraud.
10. **Data Breach:**
    This is a leak of private data to an unsecure environment. These breaches can occur from a personal computer or a corporate server.
11. **Ransomware:**
    A type of malicious software designed to block access to a computer system until money is paid.
12. **Malware / Scareware:**
    This is software intended to damage software and computers.
13. **Virus:**
    Code capable of copying itself and having a detrimental effect, such as corrupting the system or destroying data.

Impacts and Losses of Internet Fraud

The top types of internet fraud by frequency are Non-Payment / Non-Delivery, Personal Data Breach, and Phishing. However, the top three internet fraud types with the highest reported loss were BEC, Confidence/Romance fraud, and Non-Payment / Non-Delivery. While Internet fraud may occur anytime and to anyone, weekdays are the most active time for fraud cases and they typically occur around 3am (regardless of time zone). Alaska has the highest billing address Fraud while Delaware has the most shipping address fraud. \

Purchases between $0-$25 are two times more likely to involve nefarious activity because internet fraud criminals try to hide their fraud with low cost items or services.

Once Internet fraud takes place, it can be challenging to determine who was behind the fraud and how to retrieve lost funds. Fortunately, there are some steps consumers can take to help prevent fraud in the first place, as well as strategies to rectify the situation after it occurs.

Preventing Internet Fraud and Remedies for Correcting It

The best course of action to prevent Internet fraud is to be safe while online. Choose your passwords carefully to not be easily guessed and be sure to change your passwords frequently. As a general rule of thumb, do not share your password with others. It is also necessary to pay close attention to the emails and texts you receive and be highly skeptical of those that come from sources with which you are not familiar.

The fewer places and organizations that have your personal information the better. Be cautious about logging into the internet from public places and always look for the lock symbol on an internet address. Avoid using any public internet locations if you are shopping online or doing online banking. If you suspect internet fraud might have occurred, you can report it to the FBI's Internet Crime Complaint Center (IC3), the Federal Trade Commission (FTC), or the Department of Justice (DOJ)

Since some scams are so well organized and convincing, and people behind them are difficult to catch. It is imperative to always keep our guard up when using technology for everyday tasks. Stay informed about the latest scamming strategies and help educate your friends and family.

Top Resources

Below are several additional resources related to internet fraud and methods for prevention.

Preventing Digital Fraud*

Latest Internet Crime Report Released*

Understanding Internet Fraud*

Reporting Internet Crime*

*You will be linking to another website not owned or operated by the bank. We are not responsible for the availability or content of this website and do not represent either the linked website or you, should you enter into a transaction. You are encouraged to review the privacy and security policies which may differ from ours.