SCAMS AND SAFETY

Internet Fraud

Internet fraud is the use of Internet services or software with Internet access to defraud victims or to otherwise take advantage of them. Internet crime schemes steal millions of dollars each year from victims and continue to plague the Internet through various methods. Several high-profile methods include the following:

- **Business E-Mail Compromise (BEC):** A sophisticated scam targeting businesses working with foreign suppliers and companies that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.
- **Data Breach:** A leak or spill of data which is released from a secure location to an untrusted environment. Data breaches can occur at the personal and corporate levels and involve sensitive, protected, or confidential information that is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so.
- **Denial of Service:** An interruption of an authorized user's access to any system or network, typically one caused with malicious intent.
- **E-Mail Account Compromise (EAC):** Similar to BEC, this scam targets the general public and professionals associated with, but not limited to, financial and lending institutions, real estate companies, and law firms. Perpetrators of EAC use compromised e-mails to request payments to fraudulent locations.
- **Malware/Scareware:** Malicious software that is intended to damage or disable computers and computer systems. Sometimes scare tactics are used by the perpetrators to solicit funds from victims.
- **Phishing/Spoofing:** Both terms deal with forged or faked electronic documents. Spoofing generally refers to the dissemination of e-mail which is forged to appear as though it was sent by someone other than the actual source. Phishing, also referred to as vishing, smishing, or pharming, is often used in conjunction with a spoofed e-mail. It is the act of sending an e-mail falsely claiming to be an established legitimate business in an attempt to deceive the unsuspecting recipient into divulging personal, sensitive information such as passwords, credit card numbers, and bank account information after directing the user to visit a specified website. The

website, however, is not genuine and was set up only as an attempt to steal the user's information.

- **Ransomware:** A form of malware targeting both human and technical weaknesses in organizations and individual networks in an effort to deny the availability of critical data and/or systems. Ransomware is frequently delivered through spear phishing emails to end users, resulting in the rapid encryption of sensitive files on a corporate network. When the victim organization determines they are no longer able to access their data, the cyber perpetrator demands the payment of a ransom, typically in virtual currency such as Bitcoin, at which time the actor will purportedly provide an avenue to the victim to regain access to their data.

Frequent instances of Internet fraud include business fraud, credit card fraud, internet auction fraud, investment schemes, Nigerian letter fraud, and non-delivery of merchandise. For information on the most common complaints and scams, see the annual reports of the Internet Crime Complaint Center (IC3), a partnership of the FBI and the National White Collar Crime Center. Also see its information on Internet Crime Schemes and its Internet Crime Prevention Tips.

Use our online tips form or the IC3 website to report potential cases of Internet fraud.