4th page

Cybercrime

Cybercrime is a crime that involves a computer and a network.[1][2] The computer may have been used in the commission of a crime, or it may be the target.[3] Cybercrime may harm someone's security and financial health.[4][5]

There are many privacy concerns surrounding cybercrime when confidential information is intercepted or disclosed, lawfully or otherwise. Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Cybercrimes crossing international borders and involving the actions of at least one nation-state are sometimes referred to as cyberwarfare. Warren Buffett describes cybercrime as the "number one problem with mankind"[6] and "poses real risks to humanity."[7]

A report (sponsored by McAfee) published in 2014 estimated that the annual damage to the global economy was $445 billion.[8] Approximately $1.5 billion was lost in 2012 to online credit and debit card fraud in the US.[9] In 2018, a study by the Center for Strategic and International Studies (CSIS), in partnership with McAfee, concludes that nearly one percent of global GDP, close to $600 billion, is lost to cybercrime each year.[10] The World Economic Forum 2020 Global Risk report confirmed that organized Cybercrimes bodies are joining forces to perpetrate criminal activities online while estimating the likelihood of their detection and prosecution to be less than 1 percent in the US.[11]

ClassificationsEdit

With traditional crime reducing, global communities continue to witness a sporadic growth in cybercrime.[12] Computer crime encompasses a broad range of activities, from financial crimes to scams, through cybersex trafficking and ad frauds [13][14]

Financial fraud crimesEdit

Main article: Internet fraud

Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. In this context, the fraud will result in obtaining a benefit by:

Altering in an unauthorized way. This requires little technical expertise and is a common form of theft by employees altering the data before entry or entering false data, or by entering unauthorized instructions or using unauthorized processes;

Altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions. This is difficult to detect;

Altering or deleting stored data;[15]

Other forms of fraud may be facilitated using computer systems, including bank fraud, carding, identity theft, extortion, and theft of classified information. These types of crime often result in the loss of private information or monetary information.

CyberterrorismEdit

Main article: Cyberterrorism

Government officials and information technology security specialists have documented a significant increase in Internet problems and server scams since early 2001. There is a growing concern among government agencies such as the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) that such intrusions are part of an organized effort by cyberterrorist foreign intelligence services, or other groups to map potential security holes in critical systems.[16] A cyberterrorist is someone who intimidates or coerces a government or an organization to advance his or her political or social objectives by launching a computer-based attack against computers, networks, or the information stored on them.

Cyberterrorism, in general, can be defined as an act of terrorism committed through the use of cyberspace or computer resources (Parker 1983). As such, a simple propaganda piece on the Internet that there will be bomb attacks during the holidays can be considered cyberterrorism. There are also hacking activities directed towards individuals, families, organized by groups within networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruining peoples' lives, robberies, blackmailing, etc.[17]

CyberextortionEdit

Main article: Extortion

Cyberextortion occurs when a website, e-mail server, or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. These hackers demand money in return for promising to stop the attacks and to offer "protection". According to the Federal Bureau of Investigation, cybercrime extortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service. More than 20 cases are reported each month to the FBI and many go unreported in order to keep the victim's name out of the public domain. Perpetrators typically use a distributed denial-of-service attack.[18] However, other cyberextortion techniques exist such as doxing extortion and bug poaching.

An example of cyberextortion was the attack on Sony Pictures of 2014.[19]

Ransomware is a kind of cyberextortion in which a malware is used to restrict access to files, sometimes threatening permanent data erasure unless a ransom is paid. Kapersky Lab 2016 Security Bulletin report estimates that a business falls victim of Ransomware every 40 minutes.[20] and predicted to attack a business every 11 minutes in 2021. With Ransomware remaining one of the fastest growing cybercrimes in the world, global Ransomware damage is predicted to cost up to $20 billion in 2021.[21]

Cybersex traffickingEdit

Main article: Cybersex trafficking

Cybersex trafficking is the transportation of victims and then the live streaming of coerced sexual acts and or rape on webcam.[22][23][24][25] Victims are abducted, threatened, or deceived and transferred to 'cybersex dens.'[26][27][28] The dens can be in any location where the cybersex traffickers have a computer, tablet, or phone with internet connection.[24] Perpetrators use social media networks, videoconferences, dating pages, online chat rooms, apps, dark web sites,[29] and other platforms.[30] They use online payment systems[29][31][32] and cryptocurrencies to hide their identities.[33] Millions of reports of its occurrence are sent to authorities annually.[34] New legislation and police procedures are needed to combat this type of cybercrime.[35]

An example of cybersex trafficking is the 2018–2020 Nth room case in South Korea.[36]

CyberwarfareEdit

Main article: Cyberwarfare

The U.S. Department of Defense notes that the cyberspace has emerged as a national-level concern through several recent events of geostrategic significance. Among those are included, the attack on Estonia's infrastructure in 2007, allegedly by Russian hackers. In August 2008, Russia again allegedly conducted cyber attacks, this time in a coordinated and synchronized kinetic and non-kinetic campaign against the country of Georgia. Fearing that such attacks may become the norm in future warfare among nation-states, the concept of cyberspace operations impacts and will be adapted by warfighting military commanders in the future.[37]

Computer as a targetEdit

These crimes are committed by a selected group of criminals. Unlike crimes using the computer as a tool, these crimes require the technical knowledge of the perpetrators. As such, as technology evolves, so too does the nature of the crime. These crimes are relatively new, having been in existence for only as long as computers have—which explains how unprepared society and the world, in general, is towards combating these crimes. There are numerous crimes of this nature committed daily on the internet. It is seldom committed by loners, instead it involves large syndicate groups.

Crimes that primarily target computer networks include:

Computer viruses

Denial-of-service attacks

Malware (malicious code)

Computer as a toolEdit

Main articles: Internet fraud, Spamming, Phishing, and Carding (fraud)

When the individual is the main target of cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise. Human weaknesses are generally exploited. The damage dealt is largely psychological and intangible, making legal action against the variants more difficult. These are the crimes which have existed for centuries in the offline world. Scams, theft, and the likes have existed even before the development in high-tech equipment. The same criminal has simply been given a tool which increases their potential pool of victims and makes them all the harder to trace and apprehend.[38]

Crimes that use computer networks or devices to advance other ends include:

Fraud and identity theft (although this increasingly uses malware, hacking or phishing, making it an example of both "computer as target" and "computer as tool" crime)

Information warfare

Phishing scams

Spam

Propagation of illegal obscene or offensive content, including harassment and threats

The unsolicited sending of bulk email for commercial purposes (spam) is unlawful in some jurisdictions.

Phishing is mostly propagated via email. Phishing emails may contain links to other websites that are affected by malware.[39] Or, they may contain links to fake online banking or other websites used to steal private account information.

Obscene or offensive contentEdit

The content of websites and other electronic communications may be distasteful, obscene or offensive for a variety of reasons. In some instances, these communications may be illegal.

The extent to which these communications are unlawful varies greatly between countries, and even within nations. It is a sensitive area in which the courts can become involved in arbitrating between groups with strong beliefs.

One area of Internet pornography that has been the target of the strongest efforts at curtailment is child pornography, which is illegal in most jurisdictions in the world. Debarati Halder and K. Jaishankar further define cybercrime from the perspective of gender and defined 'cybercrime against women' as "Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones".[40]

Ad-fraudEdit

See also: Ad fraud and Click fraud

Ad-frauds are particularly popular among cybercriminals, as such frauds are less likely to be prosecuted and are particularly lucrative cybercrimes.[41] Jean-Loup Richet, Professor at the Sorbonne Business School, classified the large variety of ad-fraud observed in cybercriminal communities into three categories: (1) identity fraud; (2) attribution fraud; and (3) ad-fraud services.[14]

Identity fraud aims to impersonate real users and inflate audience numbers. Several ad-fraud techniques relate to this category and include traffic from bots (coming from a hosting company or a data center, or from compromised devices); cookie stuffing; falsifying user characteristics, such as location and browser type; fake social traffic (misleading users on social networks into visiting the advertised website); and the creation of fake social signals to make a bot look more legitimate, for instance by opening a Twitter or Facebook account.

Attribution fraud aims to impersonate real users' behaviors (clicks, activities, conversations, etc.). Multiple ad-fraud techniques belong to this category: hijacked devices and the use of infected users (through a malware) as part of a botnet to participate in ad fraud campaigns; click farms (companies where low-wage employees are paid to click or engage in conversations and affiliates' offers); incentivized browsing; video placement abuse (delivered in display banner slots); hidden ads (that will never be viewed by real users); domain spoofing (ads served on a website other than the advertised real-time bidding website); and clickjacking (user is forced to click on the ad).

Ad fraud services are related to all online infrastructure and hosting services that might be needed to undertake identity or attribution fraud . Services can involve the creation of spam websites (fake networks of websites created to provide artificial backlinks); link building services; hosting services; creation of fake and scam pages impersonating a famous brand and used as part of an ad fraud campaign.

A successful ad-fraud campaign involves a sophisticated combination of these three types of ad-fraud—sending fake traffic through bots using fake social accounts and falsified cookies; bots will click on the ads available on a scam page that is faking a famous brand.

Online harassmentEdit

See also: Cyberbullying, Online predator, Cyberstalking, Cyber Racism, and Internet troll

Learn more

The examples and perspective in this section **may not represent a worldwide view of the subject**. (March 2016)

Whereas content may be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing for example on gender, race, religion, nationality, sexual orientation.

There are instances where committing a crime using a computer can lead to an enhanced sentence. For example, in the case of United States v. Neil Scott Kramer, the defendant was given an enhanced sentence according to the U.S. Sentencing Guidelines Manual §2G1.3(b)(3) for his use of a cell phone to "persuade, induce, entice, coerce, or facilitate the travel of, the minor to engage in prohibited sexual conduct." Kramer appealed the sentence on the grounds that there was insufficient evidence to convict him under this statute because his charge included persuading through a computer device and his cellular phone technically is not a computer. Although Kramer tried to argue this point, the U.S. Sentencing Guidelines Manual states that the term 'computer' "means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

In the United States alone, Missouri and over 40 other states have passed laws and regulations that regard extreme online harassment as a criminal act. These acts can be punished on a federal scale, such as US Code 18 Section 2261A, which states that using computers to threaten or harass can lead to a sentence of up to 20 years, depending on the action taken.[42]

Several countries outside of the United States have also created laws to combat online harassment. In China, a country that supports over 20 percent of the world's internet users, the Legislative Affairs Office of the State Council passed a strict law against the bullying of young people through a bill in response to the Human Flesh Search Engine.[43][44] The United Kingdom passed the Malicious Communications Act, among other acts from 1997 to 2013, which stated that sending messages or letters electronically that the government deemed "indecent or grossly offensive" and/or language intended to cause "distress and anxiety" can lead to a prison sentence of six months and a potentially large fine.[45][46] Australia, while not directly addressing the issue of harassment, has grouped the majority of online harassment under the Criminal Code Act of 1995. Using telecommunication to send threats or harass and cause offense was a direct violation of this act.[47]

Although freedom of speech is protected by law in most democratic societies (in the US this is done by the First Amendment), it does not include all types of speech. In fact, spoken or written "true threat" speech/text is criminalized because of "intent to harm or intimidate." That also applies for online or any type of network-related threats in written text or speech.

Cyberbullying has increased drastically with the growing popularity of online social networking. As of January 2020, 44% of adult internet users in the United States have "personally experienced online harassment."[48] Children who experience online harassment deal with negative and sometimes life-threatening side effects. In 2021, reports displayed 41% of children developing social anxiety, 37% of children developing depression, and 26% of children having suicidal thoughts.[49]

The United Arab Emirates was named in a spying scandal where the Gulf nation along with other repressive governments purchased NSO Group’s mobile spyware Pegasus for mass surveillance. Prominent activists and journalists were targeted as part of the campaign, including, Ahmed Mansoor, Princess Latifa, Princess Haya, and more. Ghada Oueiss was one of the many high-profile female journalists and activists who became the target of online harassment. Oueiss filed a lawsuit against the UAE ruler, Mohamed bin Zayed Al Nahyan along with other defendants, accusing them of sharing her photos online. The defendants including the UAE ruler filed motions to dismiss the case of the hack-and-leak attack.[50]

Drug traffickingEdit

Darknet markets are used to buy and sell recreational drugs online. Some drug traffickers use encrypted messaging tools to communicate with drug mules. The dark web site Silk Road was a major online marketplace for drugs before it was shut down by law enforcement (then reopened under new management, and then shut down by law enforcement again). After Silk Road 2.0 went down, Silk Road 3 Reloaded emerged. However, it was just an older marketplace named Diabolus Market, that used the name for more exposure from the brand's previous success.[51]

Darknet markets have had an up-rise in traffic in recent years for many reasons. One of the biggest contributors being the anonymity and safety that goes along when using the markets.[52] There are numerous ways you can lose all your money invested and be caught when using Darknet markets. Vendors and customers alike go to great lengths to keep their identities a secret while online. Commonly used tools are virtual private networks, Tails, and Tor to help hide their trail left behind for investigators. Darknet markets make the user feel safe as they can get what they want from the comfort of their home. People can easily gain access to a Tor browser with DuckDuckGo browser that allows a user to explore much deeper than other browsers such as Google Chrome. However actually gaining access to an illicit market isn't as simple as typing it in on the search engine like you would with google. Darknet markets have special links that are changing everyday ending in .onion opposed to the typical .com, .net. and .org domain extensions. To add to privacy the biggest currency on these markets is Bitcoin. Bitcoin allows transactions to be committed between people by exchanging wallet addresses and never having to know anything about the person you're sending money to.[53]

One of the biggest issues the users face who use marketplaces are the vendors or market itself exit scamming.[54] This is when usually a vendor with a high rating will act as if they're still selling on the market and have users send them money.[55] The vendor will then close off his account after receiving money from multiple buyers and never send what they purchased. The vendors all being involved in illegal activities have a low chance at not exit scamming when they no longer want to be a vendor. In 2019, an entire market called Wall Street Market had allegedly exit scammed, stealing 30 million dollars from the vendors and buyers wallets in bitcoin.[56]

Federal agents have had a huge crackdown on these markets. In July 2017, federal agents seized one of the biggest markets commonly called Alphabay which ironically later re-opened in August 2021 under the control of one of the original administrators DeSnake.[57][58] Commonly investigators will pose as a buyer and order packages from darknet vendors in the hopes they left a trail they can follow. One investigation had an investigator pose as a firearms seller and for six months people purchased from them and provided home addresses.[59] They were able to make over a dozen arrests during this six-month investigation.[59] Another one of law enforcement's biggest crackdowns are on vendors selling fentanyl and opiates. With thousands of dying each year due to drug over dose it was long overdue for law enforcement to crack down on these markets.[60] Many vendors don't realize the extra charges that go along with selling drugs online. Commonly they get charged with money laundering and charges for when the drugs are shipped in the mail on top of being a drug distributor.[61] Each state has its laws and regulations on drugs therefore vendors have the face multiple charges from different states. In 2019, a vendor was sentenced to 10 years in prison after selling cocaine and methamphetamine under the name JetSetLife.[62] Although many investigators spend a lot of time tracking down people in the course of a year only 65 suspects were identified who bought and sold illegal goods on some of the biggest markets.[63] This is compared to the thousands of transactions taking place daily on these markets.

One of the highest profiled banking computer crime occurred during a course of three years beginning in 1970. The chief teller at the Park Avenue branch of New York's Union Dime Savings Bank embezzled over $1.5 million from hundreds of accounts.[64]

A hacking group called MOD (Masters of Deception), allegedly stole passwords and technical data from Pacific Bell, Nynex, and other telephone companies as well as several big credit agencies and two major universities. The damage caused was extensive, one company, Southwestern Bell suffered losses of $370,000 alone.[64]

In 1983, a 19-year-old UCLA student used his PC to break into a Defense Department International Communications system.[64]

Between 1995 and 1998 the Newscorp satellite pay to view encrypted SKY-TV service was hacked several times during an ongoing technological arms race between a pan-European hacking group and Newscorp. The original motivation of the hackers was to watch Star Trek reruns in Germany; which was something which Newscorp did not have the copyright to allow.[65]

On 26 March 1999, the Melissa worm infected a document on a victim's computer, then automatically sent that document and a copy of the virus spread via e-mail to other people.

In February 2000, an individual going by the alias of MafiaBoy began a series denial-of-service attacks against high-profile websites, including Yahoo!, Dell, Inc., E*TRADE, eBay, and CNN. About 50 computers at Stanford University, and also computers at the University of California at Santa Barbara, were amongst the zombie computers sending pings in DDoS attacks. On 3 August 2000, Canadian federal prosecutors charged MafiaBoy with 54 counts of illegal access to computers, plus a total of ten counts of mischief to data for his attacks.

The Stuxnet worm corrupted SCADA microprocessors, particularly of the types used in Siemens centrifuge controllers.

The Flame (malware) that mainly targeted Iranian officials in an attempt to obtain sensitive information.[66]

The Russian Business Network (RBN) was registered as an internet site in 2006. Initially, much of its activity was legitimate. But apparently, the founders soon discovered that it was more profitable to host illegitimate activities and started hiring its services to criminals. The RBN has been described by VeriSign as "the baddest of the bad".[67] It offers web hosting services and internet access to all kinds of criminal and objectionable activities, with individual activities earning up to $150 million in one year. It specialized in and in some cases monopolized personal identity theft for resale. It is the originator of MPack and an alleged operator of the now-defunct Storm botnet.

On 2 March 2010, Spanish investigators arrested 3 men who were suspected of infecting of over 13 million computers around the world. The "botnet" of infected computers included PCs inside more than half of the Fortune 1000 companies and more than 40 major banks, according to investigators.[68]

In August 2010 the international investigation Operation Delego, operating under the aegis of the Department of Homeland Security, shut down the international pedophile ring Dreamboard.

The website had approximately 600 members and may have distributed up to 123 terabytes of child pornography (roughly equivalent to 16,000 DVDs). To date this is the single largest U.S. prosecution of an international child pornography ring; 52 arrests were made worldwide.[69]

In January 2012 Zappos.com experienced a security breach after as many as 24 million customers' credit card numbers, personal information, billing and shipping addresses had been compromised.[70]

In June 2012 LinkedIn and eHarmony were attacked, compromising 65 million password hashes. 30,000 passwords were cracked and 1.5 million EHarmony passwords were posted online.[71]

December 2012 Wells Fargo website experienced a denial of service attack. Potentially compromising 70 million customers and 8.5 million active viewers. Other banks thought to be compromised: Bank of America, J. P. Morgan U.S. Bank, and PNC Financial Services.[72]

23 April 2013 saw the Associated Press' Twitter account's hacked - the hacker posted a hoax tweet about fictitious attacks in the White House that they claimed left President Obama injured.[73] This hoax tweet resulted in a brief plunge of 130 points from the Dow Jones Industrial Average, removal of $136 billion from S&P 500 index,[74] and the temporary suspension of AP's Twitter account. The Dow Jones later restored its session gains.

In May 2017, 74 countries logged a ransomware cybercrime, called "WannaCry"[75]

Illicit access to camera sensors, microphone sensors, phonebook contacts, all internet-enabled apps, and metadata of mobile telephones running Android and IOS were reportedly made accessible by Israeli spyware, found to be being in operation in at least 46 nation-states around the world. Journalists, Royalty and government officials were amongst the targets.[76][77][78] Previous accusations of cases of Israeli-weapons companies meddling in international telephony[79] and smartphones[80] have been eclipsed in the 2018 reported case.

In December 2019, the United States intelligence and an investigation by The New York Times revealed that messaging application of the United Arab Emirates, ToTok is a spying tool. The research revealed that the Emirati government attempted to track every conversation, movement, relationship, appointment, sound and image of those who install the app on their phones.[

had an up-rise in traffic in recent years for many reasons. One of the biggest contributors being the anonymity and safety that goes along when using the markets.[52] There are numerous ways you can lose all your money invested and be caught when using Darknet markets. Vendors and customers alike go to great lengths to keep their identities a secret while online. Commonly used tools are virtual private networks, Tails, and Tor to help hide their trail left behind for investigators. Darknet markets make the user feel safe as they can get what they want from the comfort of their home. People can easily gain access to a Tor browser with DuckDuckGo browser that allows a user to explore much deeper than other browsers such as Google Chrome. However actually gaining access to an illicit market isn't as simple as typing it in on the search engine like you would with google. Darknet markets have special links that are changing everyday ending in .onion opposed to the typical .com, .net. and .org domain extensions. To add to privacy the biggest currency on these markets is Bitcoin. Bitcoin allows transactions to be committed between people by exchanging wallet addresses and never having to know anything about the person you're sending money to.[53]

One of the biggest issues the users face who use marketplaces are the vendors or market itself exit scamming.[54] This is when usually a vendor with a high rating will act as if they're still selling on the market and have users send them money.[55] The vendor will then close off his account after receiving money from multiple buyers and never send what they purchased. The vendors all being involved in illegal activities have a low chance at not exit scamming when they no longer want to be a vendor. In 2019, an entire market called Wall Street Market had allegedly exit scammed, stealing 30 million dollars from the vendors and buyers wallets in bitcoin.[56]

Federal agents have had a huge crackdown on these markets. In July 2017, federal agents seized one of the biggest markets commonly called Alphabay which ironically later re-opened in August 2021 under the control of one of the original administrators DeSnake.[57][58] Commonly investigators will pose as a buyer and order packages from darknet vendors in the hopes they left a trail they can follow. One investigation had an investigator pose as a firearms seller and for six months people purchased from them and provided home addresses.[59] They were able to make over a dozen arrests during this six-month investigation.[59] Another one of law enforcement's biggest crackdowns are on vendors selling fentanyl and opiates. With thousands of dying each year due to drug over dose it was long overdue for law enforcement to crack down on these markets.[60] Many vendors don't realize the extra charges that go along with selling drugs online. Commonly they get charged with money laundering and charges for when the drugs are shipped in the mail on top of being a drug distributor.[61] Each state has its laws and regulations on drugs therefore vendors have the face multiple charges from different states. In 2019, a vendor was sentenced to 10 years in prison after selling cocaine and methamphetamine under the name JetSetLife.[62] Although many investigators spend a lot of time tracking down people in the course of a year only 65 suspects