Click Here

, the free encyclopedia that anyone can edit. 110,144 active editors 7,022,728 articles in English Sirius A with Sirius B, a white dwarf, indicated by the arrow A white dwarf is a stellar core remnant composed mostly of electron-degenerate matter, supported against its own gravity only by electron degeneracy pressure. A white dwarf is very dense: in an Earth sized volume, it contains a mass comparable to the Sun. What light it radiates is from its residual heat. White dwarfs are thought to be the final evolutionary state of stars whose mass is insufficient for them to become a neutron star or black hole. This includes more than 97% of the stars in the Milky Way. After the hydrogen-fusing period of such a main-sequence star ends, it will expand to a red giant and shed its outer layers, leaving behind a core which is the white dwarf. This, very hot when it forms, cools as it radiates its energy until its material begins to crystallize into a cold black dwarf. The oldest known white dwarfs still radiate at temperatures of a few thousand kelvins, which establishes an observational limit on the maximum possible age of the universe. (Full article...) Recently featured: Battle of Groix Scott Carpenter Johann Reinhold Forster Archive By email More featured articles About A Royal 10 typewriter ... that a Royal 10 (pictured) used in the music video for "Fortnight" caused an interest in typewriters among Swifties? ... that the Brazilian government advocated the use of COVID kits, which contained a drug used to treat head lice? ... that Brave Bunnies was among the children's series streamed ad-free on Sunflower TV for Ukrainian refugees? ... that it took more than two years after the Romans invaded Africa in 204 BC for them to completely defeat the Carthaginians? ... that the Pittsburgh Post-Gazette reported that "half of the residents of Mount Desert Island, Maine, are convinced they are millionaires since the body of Karl N. Mellon" was discovered? ... that AiScReam's recent debut song "Ai Scream!" went viral on social media? ... that Laura LeRoy Travis was the first woman at the University of Delaware to coach a men's sports team? ... that the screenplay for Smashing Frank was developed from an assignment in a filmmaking course? ... that the iconic 1937 photograph At the Time of the Louisville Flood identifiably depicts neither Louisville nor the flood? Archive Start a new article Nominate an article Vera Rubin Observatory The Vera C. Rubin Observatory (pictured) in Chile releases the first light images from its new 8.4-metre (28 ft) telescope. In basketball, the Oklahoma City Thunder defeat the Indiana Pacers to win the NBA Finals. The United States conducts military strikes on three nuclear facilities in Iran. In rugby union, the Crusaders defeat the Chiefs to win the Super Rugby Pacific final. In ice hockey, the Florida Panthers defeat the Edmonton Oilers to win the Stanley Cup. Ongoing: Gaza war Iran–Israel war Russian invasion of Ukraine timeline Sudanese civil war timeline Recent deaths: Frederick W. Smith Ron Taylor Mohammad Kazemi Marita Camacho Quirós Kim Woodburn William Langewiesche Nominate an article June 24: Jaanipäev in Estonia Julia Gillard 1374 – An outbreak of dancing mania, in which crowds of people danced themselves to exhaustion, began in Aachen (in present-day Germany) before spreading to other parts of Europe. 1717 – The first Grand Lodge of Freemasonry, the Premier Grand Lodge of England, was founded in London. 1724 – On the Feast of St. John the Baptist, Bach led the first performance of Christ unser Herr zum Jordan kam, BWV 7, the third cantata of his chorale cantata cycle. 1943 – Amid racial tensions, U.S. Army military police shot and killed a black serviceman after a confrontation at a pub in Bamber Bridge, England. 2010 – Julia Gillard (pictured) was sworn in as the first female prime minister of Australia after incumbent Kevin Rudd declined to contest a leadership spill in the Labor Party. William Arnold (b. 1587)John Lloyd Cruz (b. 1983)Lisa (b. 1987)Rodrigo (d. 2000) More anniversaries: June 23 June 24 June 25 Archive By email List of days of the year About The springbok (Antidorcas marsupialis) is a medium-sized antelope found mainly in the dry areas of southern and southwestern Africa. A slender, long-legged bovid, it reaches 71 to 86 cm (28 to 34 in) at the shoulder and weighs between 27 and 42 kg (60 and 93 lb). Both sexes have a pair of long black horns that curve backwards, a white face, a dark stripe running from the eyes to the mouth, a light-brown coat with a reddish-brown stripe, and a white rump flap. Primarily browsing at dawn and dusk, it can live without drinking water for years, subsisting on succulent vegetation. Breeding peaks in the rainy season, when food is more abundant. A single calf is weaned at nearly six months of age and leaves its mother a few months later. Springbok herds in the Kalahari Desert and the semi-arid Karoo used to migrate in large numbers across the countryside. The springbok is the national animal of South Africa. This male springbok was photographed in Etosha National Park, Namibia. Photograph credit: Yathin S Krishnappa Recently featured: Geraldine Ulmar Shah Mosque (Isfahan) Cape Barren goose Archive More featured pictures Community portal – The central hub for editors, with resources, links, tasks, and announcements. Village pump – Forum for discussions about Wikipedia itself, including policies and technical issues. Site news – Sources of news about Wikipedia and the broader Wikimedia movement. Teahouse – Ask basic questions about using or editing Wikipedia. Help desk – Ask questions about using or editing Wikipedia. Reference desk – Ask research questions about encyclopedic topics. Content portals – A unique way to navigate the encyclopedia. Wikipedia is written by volunteer editors and hosted by the Wikimedia Foundation, a non-profit organization that also hosts a range of other volunteer projects: CommonsFree media repository MediaWikiWiki software development Meta-WikiWikimedia project coordination WikibooksFree textbooks and manuals WikidataFree knowledge base WikinewsFree-content news WikiquoteCollection of quotations WikisourceFree-content library WikispeciesDirectory of species WikiversityFree learning tools WikivoyageFree travel guide WiktionaryDictionary and thesaurus This Wikipedia is written in English. Many other Wikipedias are available; some of the largest are listed below. 1,000,000+ articles العربية Deutsch Español فارسی Français Italiano Nederlands 日本語 Polski Português Русский Svenska Українська Tiếng Việt 中文 250,000+ articles Bahasa Indonesia Bahasa Melayu Bân-lâm-gú Български Català Čeština Dansk Eesti Ελληνικά Esperanto Euskara עברית Հայերեն Magyar Norsk bokmål Română Simple English Slovenčina Srpski Srpskohrvatski Suomi Türkçe Oʻzbekcha 50,000+ articles Asturianu Azərbaycanca □□□□□ Bosanski کوردی Frysk Gaeilge Galego Hrvatski ქართული Kurdî Latviešu Lietuvių □□□□□ Македонски □□□□□□□□□□ Norsk nynorsk □□□□□ Shqip Slovenščina □□□ □□□□□ اردو Retrieved from " 2 This article needs additional citations for verification. Please help improve this article by adding citations to reliable sources. Unsourced material may be challenged and removed.Find sources: "1374" – news · newspapers · books · scholar · JSTOR (June 2017) (Learn how and when to remove this message) Calendar year Years Millennium 2nd millennium Centuries 13th century 14th century 15th century Decades 1350s 1360s 1370s 1380s 1390s Years 1371 1372 1373 1374 1375 1376 1377 vte 1374 by topic Leaders Political entities State leaders Religious leaders Birth and death categories Births – Deaths Establishments and disestablishments categories Establishments – Disestablishments Art and literature 1374 in poetry vte 1374 in various calendarsGregorian calendar1374MCCCLXXIVAb urbe condita2127Armenian calendar823ԹՎ ՊԻԳAssyrian calendar6124Balinese saka calendar1295–1296Bengali calendar780–781Berber calendar2324English Regnal year47 Edw. 3 – 48 Edw. 3Buddhist calendar1918Burmese calendar736Byzantine calendar6882–6883Chinese calendar癸丑年 (Water Ox)4071 or 3864 — to —甲寅年 (Wood Tiger)4072 or 3865Coptic calendar1090–1091Discordian calendar2540Ethiopian calendar1366–1367Hebrew calendar5134–5135Hindu calendars - Vikram Samvat1430–1431 - Shaka Samvat1295–1296 - Kali Yuga4474–4475Holocene calendar11374Igbo calendar374–375Iranian calendar752–753Islamic calendar775–776Japanese calendarŌan 7(応安７年)Javanese calendar1287–1288Julian calendar1374MCCCLXXIVKorean calendar3707Minguo calendar538 before ROC民前538年Nanakshahi calendar−94Thai solar calendar1916–1917Tibetan calendar阴水牛年(female Water-Ox)1500 or 1119 or 347 — to —阳木虎年(male Wood-Tiger)1501 or 1120 or 348Year 1374 (MCCCLXXIV) was a common year starting on Sunday of the Julian calendar. April 23 – In recognition of his services, Edward III of England grants the English writer Geoffrey Chaucer a gallon of wine a day, for the rest of his life. June 24 – The illness dancing mania begins in Aix-la-Chapelle (Aachen), possibly due to ergotism. October 27 – King Gongmin of Goryeo is assassinated and succeeded by U of Goryeo on the throne of Goryeo (in modern-day Korea). November 25 – James of Baux succeeds his uncle, Philip II, as Prince of Taranto (modern-day eastern Italy) and titular ruler of the Latin Empire (northern Greece and western Turkey). Rao Biram Dev succeeds Rao Kanhadev as ruler of Marwar (the modern-day Jodhpur district of India). Shaikh Hasan Jalayir succeeds his father, Shaykh Uways Jalayir, as ruler of the Jalayirid Sultanate in modern-day Iraq and western Iran. Hasan proves to be an unpopular ruler and is executed on October 9 and succeeded by his brother, Shaikh Hussain Jalayir. Musa II succeeds his father, Mari Djata II, as Mansa of the Mali Empire (modern-day Mali and Senegal). Robert de Juilly succeeds Raymond Berenger as Grand Master of the Knights Hospitaller. Princes from the Kingdom of Granada choose Abu al-Abbas Ahmad to succeed Muhammad as-Said, as Sultan of the Marinid Empire in Morocco. The Empire is split into the Kingdom of Fez and the Kingdom of Marrakech. A form of the Great Plague returns to Europe. The Château de Compiègne royal residence is built in France. April 11 – Roger Mortimer, 4th Earl of March, heir to the throne of England (d. 1398) November 26 – Yury Dmitrievich, Russian grand prince (d. 1434) probable Queen Jadwiga of Poland King Martin I of Sicily (d. 1409) March 12 – Emperor Go-Kōgon of Japan (b. 1338). June 5 or June 6 – William Whittlesey, Archbishop of Canterbury June 29 – Jan Milíč of Kroměříž, Czech priest and reformer July 19 – Petrarch, Italian poet (b. 1304) September – Joanna of Flanders, Duchess of Brittany (b. 1295) October 27 – King Gongmin of Goryeo (b. 1330) November 25 – Prince Philip II of Taranto December 1 – Magnus Eriksson, king of Sweden (b. 1316) date unknown – Gao Qi, Chinese poet (born 1336) date unknown – Konrad of Megenberg, historian (b. 1309)[1] ^ "Book of Nature". World Digital Library. August 7, 2013. Retrieved August 27, 2013. Retrieved from " 3One hundred years, from 1201 to 1300 For the video game series, see XIII Century (series). Millennia 2nd millennium Centuries 12th century 13th century 14th century Timelines 12th century 13th century 14th century State leaders 12th century 13th century 14th century Decades 1200s 1210s 1220s 1230s 1240s 1250s 1260s 1270s 1280s 1290s Categories: Births – Deaths Establishments – Disestablishments vte Mongol Emperor Genghis Khan whose conquests created the largest contiguous empire in history The 13th century was the century which lasted from January 1, 1201 (represented by the Roman numerals MCCI) through December 31, 1300 (MCCC) in accordance with the Julian calendar. The Mongol Empire was founded by Genghis Khan, which stretched from Eastern Asia to Eastern Europe. The conquests of Hulagu Khan and other Mongol invasions changed the course of the Muslim world, most notably the Siege of Baghdad (1258) and the destruction of the House of Wisdom. Other Muslim powers such as the Mali Empire and Delhi Sultanate conquered large parts of West Africa and the Indian subcontinent, while Buddhism witnessed a decline through the conquest led by Bakhtiyar Khilji. The earliest Islamic states in Southeast Asia formed during this century, most notably Samudera Pasai.[1] The Kingdoms of Sukhothai and Hanthawaddy would emerge and go on to dominate their surrounding territories.[2] Europe entered the apex of the High Middle Ages, characterized by rapid legal, cultural, and religious evolution as well as economic dynamism. Crusades after the fourth, while mostly unsuccessful in rechristianizing the Holy Land, inspired the desire to expel Muslim presence from Europe that drove the Reconquista and solidified a sense of Christendom. To the north, the Teutonic Order Christianized and gained dominance of Prussia, Estonia, and Livonia. Inspired by new translations into Latin of classical works preserved in the Islamic World for over a thousand years, Thomas Aquinas developed Scholasticism, which dominated the curricula of the new universities.[3] In England, King John signed the Magna Carta, beginning the tradition of Parliamentary advisement in England. This helped develop the principle of equality under law in European judisprudence.[4] The Southern Song dynasty began the century as a prosperous kingdom but were later invaded and annexed into the Yuan dynasty of the Mongols. The Kamakura Shogunate of Japan successfully resisted two Mongol invasion attempts in 1274 and 1281. The Korean state of Goryeo resisted a Mongol invasion, but eventually sued for peace and became a client state of the Yuan dynasty.[5] In North America, according to some population estimates, the population of Cahokia grew to be comparable to the population of 13th-century London.[6] In Peru, the Kingdom of Cuzco began as part of the Late Intermediate Period. In Mayan civilization, the 13th century marked the beginning of the Late Postclassic period. The Kanem Empire in what is now Chad reached its apex. The Solomonic dynasty in Ethiopia and the Zimbabwe Kingdom were founded. Eastern Hemisphere in 1200 AD Main article: 1200s 1202: Introduction of Liber Abaci by Fibonacci. 1202: Battle of Basian occurs on July 27, between Kingdom of Georgia and Seljuks. 1202: Battle of Mirebeau occurs on August 1, between Arthur I of Brittany and John of England. 1204: Islamization of Bengal by Bakhtiyar Khalji and oppression of Buddhism in East India. 1204: Fourth Crusade of 1202–1204 captures Zadar for Venice and sacks Byzantine Constantinople, creating the Latin Empire. 1204: Fall of Normandy from Angevin hands to the French King, Philip Augustus, end of Norman domination of France. 1205: The Battle of Adrianople occurred on April 14 between Bulgarians under Tsar Kaloyan of Bulgaria, and Crusaders under Baldwin I, (July 1172 – 1205), the first emperor of the Latin Empire of Constantinople. 1206: Genghis Khan is declared Great Khan of the Mongols. 1206: The Delhi Sultanate is established in Northern India under the Mamluk Dynasty. 1209: Francis of Assisi founds the Franciscan Order. 1209: The Albigensian Crusade is declared by Pope Innocent III. Main article: 1210s A page of the Italian Fibonacci's Liber Abaci from the Biblioteca Nazionale di Firenze showing the Fibonacci sequence with the position in the sequence labeled in Roman numerals and the value in Arabic-Hindu numerals. 1210: Qutb-ud-Din Aibak, the first ruler of the Delhi Sultanate, fell down from a horse while playing chovgan (a form of polo on horseback) in Lahore and died instantly when the pommel of the saddle pierced his ribs. 1212: The Battle of Las Navas de Tolosa in Iberia marks the beginning of a rapid Christian reconquest of the southern half of the Iberian Peninsula, mainly from 1230–1248, with the defeat of Moorish forces. 1212: Frederick of Sicily is crowned King of the Romans at Mainz. 1213: The Kingdom of France defeats the Crown of Aragon at the Battle of Muret. 1214: France defeats the English and Imperial German forces at the Battle of Bouvines. 1215: King John signs Magna Carta at Runnymede. 1216: Battle of Lipitsa between Russian principalities. 1216: Maravarman Sundara I reestablishes the Pandya Dynasty in Southern India 1217–1221: Fifth Crusade captures Egyptian Ayyubid port city of Damietta; ultimately the Crusaders withdraw. Main article: 1220s c. 1220: The Kingdom of Mapungubwe was established 1220: Frederick II, Holy Roman Emperor is crowned in Rome 1221: Merv, Herat, Bamyan and Nishapur are destroyed in the Mongol invasion of the Khwarazmian Empire. 1222: Andrew II of Hungary signs the Golden Bull which affirms the privileges of Hungarian nobility. 1223: The Signoria of the Republic of Venice is formed and consists of the Doge, the Minor Council, and the three leaders of the Quarantia. 1223: The Mongol Empire defeats various Russian principalities at the Battle of the Kalka River. 1223: Volga Bulgaria defeats the army of the Mongol Empire at the Battle of Samara Bend. 1225: Trần dynasty of Vietnam was established by Emperor Trần Thái Tông ascended to the throne after his uncle Trần Thủ Độ orchestrated the overthrow of the Lý dynasty. 1226–1250: Dispute between the so-called second Lombard League and Emperor Frederick II. 1227: Estonians are finally subjugated to German crusader rule during the Livonian Crusade. 1227: Genghis Khan dies. 1228–1229: Sixth Crusade under the excommunicated Emperor Frederick II, who returns Jerusalem to the Crusader States in a negotiated settlement with the Sultan of Egypt, Al-Kamil 1228–1230: First clash between Gregory IX and Emperor Frederick II. Main article: 1230s Portrait of the Chinese Zen Buddhist Wuzhun Shifan, painted in 1238, Song dynasty. 1231: Emperor Frederick II promulgates the Constitutions of Melfi, a far-reaching legal code influential in the development of continental European statehood.[7][8] 1232: The Mongols besiege Kaifeng, the capital of the Jin dynasty, capturing it in the following year. 1233: Battle of Ganter, Ken Arok defeated Kertajaya, the last king of Kediri, thus established Singhasari kingdom[9] Ken Arok ended the reign of Isyana Dynasty and started his own Rajasa dynasty. 1235: The Mandinka kingdoms unite to form the Mali Empire which leads to the downfall of Sosso in the 1230s. 1237: Emperor Frederick II virtually annihilates the forces of the second Lombard League at the Battle of Cortenuova. 1239–1250: Third conflict between the Holy Roman Empire and the Papacy. 1237–1240: Mongol Empire conquers Kievan Rus. 1238: Sukhothai becomes the first capital of Sukhothai Kingdom. Main article: 1240s 1240: Russians defeat the Swedish army at the Battle of the Neva. 1241: Mongol Empire defeats Hungary at the Battle of Mohi and defeats Poland at the Battle of Legnica. Hungary and Poland ravaged. 1242: Russians defeat the Teutonic Knights at the Battle of Lake Peipus. 1243–1250: Second Holy Roman Empire–Papacy War. 1244: Ayyubids and Khwarezmians defeat the Crusaders and their Muslim allies at the Battle of La Forbie. 1249: End of the Portuguese Reconquista against the Moors, when King Afonso III of Portugal reconquers the Algarve. 1248–1254: Seventh Crusade captures Egyptian Ayyubid port city of Damietta, crusaders ultimately withdraw, after the capture of French king Louis IX. Mamelukes overthrow Ayyubid Dynasty. Main article: 1250s Mongol Empire in 1227 at Genghis Khan's death By 1250, Pensacola culture, through trade, begins influencing Coastal Coles Creek culture.[10] 1250: The Mamluk dynasty is founded in Egypt. 1250: Death of Emperor Frederick II on December 13th. 1257: Baab Mashur Malamo established the Sultanate of Ternate in Maluku. 1258: Baghdad captured and destroyed by the Mongols, effective conclusion of the Abbasid Caliphate in Baghdad. 1258: Pandayan Emperor Jatavarman Sundara I invades Eastern India and northern Sri Lanka. 1259: Treaty of Paris is signed between Louis IX and Henry III Main article: 1260s 1260: Mongols first major war defeat in the Battle of Ain Jalut against the Egyptians. 1260: Toluid Civil War begins between Kublai Khan and Ariq Böke for the title of Great Khan. 1261: Byzantines under Michael VIII retake Constantinople from the Crusaders and Venice. 1262: Iceland brought under Norwegian rule, with the Old Covenant. 1265: Dominican theologian Thomas Aquinas begins to write his Summa Theologiae. 1268: Fall of the Crusader State of Antioch to the Egyptians. Main article: 1270s The opening page of one of Ibn al-Nafis' medical works. This is probably a copy made in India during the 17th or 18th century. 1270: Goryeo dynasty swears allegiance to the Yuan dynasty. 1270: The Zagwe dynasty is displaced by the Solomonic dynasty. 1271: Edward I of England and Charles of Anjou arrive in Acre, starting the Ninth Crusade against Baibars. 1272–1274: Second Council of Lyon attempts to unite the churches of the Eastern Roman Empire with the Church of Rome. 1274: The Mongols launch their first invasion of Japan, but they are repelled by the Samurai and the Kamikaze winds. 1274: The Tepanec give the Mexica permission to settle at the islet Cauhmixtitlan (Eagle's Place Between the Clouds) 1275: Sant Dnyaneshwar who wrote Dnyaneshwari (a commentary on the Bhagavad Gita) and Amrutanubhav was born. 1275: King Kertanegara of Singhasari launched Pamalayu expedition against Melayu Kingdom in Sumatra (ended in 1292). 1277: Passage of the last and most important of the Paris Condemnations by Bishop Tempier, which banned a number of Aristotelian propositions 1279: The Song dynasty ends after losing the Battle of Yamen to the Mongols. 1279: The Chola Dynasty in Southern India officially comes to an end. Main article: 1280s 1281: The Mongols launch their second invasion of Japan, but like their first invasion they are repelled by the Samurai and the Kamikaze winds. 1282: Aragon acquires Sicily after the Sicilian Vespers. 1284: Peterhouse, Cambridge founded by Hugo de Balsham, the Bishop of Ely. 1284: King Kertanegara launches the Pabali expedition to Bali, integrating Bali into the Singhasari territory. 1285: Second Mongol raid against Hungary, led by Nogai Khan. 1289: The County of Tripoli falls to the Bahri Mamluks led by Qalawun. 1289: Kertanegara insulted the envoy of Kublai Khan, who demanded that Java pay tribute to the Yuan Dynasty.[11][12] Main articles: 1290s and 1300s Hommage of Edward I (kneeling), to the Philippe le Bel (seated). As duke of Aquitaine, Edward was a vassal to the French king. The Mamluk Dynasty comes to an end and is replaced by the Khalji dynasty. 1290: By the Edict of Expulsion, King Edward I of England orders all Jews to leave the Kingdom of England. 1291: The Swiss Confederation of Uri, Schwyz, and Unterwalden forms. 1291: Mamluk Sultan of Egypt al-Ashraf Khalil captures Acre, thus ending the Crusader Kingdom of Jerusalem (the last Christian state remaining from the Crusades). 1292: Jayakatwang, duke of Kediri, rebels and kills Kertanegara, ending the Singhasari kingdom. 1292: Marco Polo, on his voyage from China to Persia, visits Sumatra and reports that, on the northern part of Sumatra, there were six trading ports, including Ferlec, Samudera and Lambri.[13] 1292: King Mangrai founds the Lanna kingdom. 1293: Mongol invasion of Java.[14] Kublai Khan of Yuan dynasty China, sends punitive attack against Kertanegara of Singhasari, who repels the Mongol forces. 1293: On 10 November, the coronation of Nararya Sangramawijaya as monarch, marks the foundation of the Hindu Majapahit kingdom in eastern Java. 1296: First War of Scottish Independence begins. 1297: Membership in the Mazor Consegio or the Great Council of Venice of the Venetian Republic is sealed and limited in the future to only those families whose names have been inscribed therein. 1299: Ottoman Empire is established under Osman I. 1300: Islam is likely established in the Aceh region. 1300: Aji Batara Agung Dewa Sakti founds the Kingdom of Kutai Kartanegara/Sultanate of Kutai in the Tepian Batu or Kutai Lama. 1300: The Turku Cathedral was consecrated in Turku.[15] 1300: Sri Rajahmura Lumaya, known in his shortened name Sri Lumay, a half-Tamil and half Malay minor prince of the Chola dynasty in Sumatra established the Indianized Rajahnate of Cebu in Cebu Island on the Philippine Archipelago. Alai Gate and Qutub Minar were built during the Mamluk and Khalji dynasties of the Delhi Sultanate.[16] Early 13th century – Xia Gui paints Twelve Views from a Thatched Hut, during the Southern Song dynasty (now in Nelson-Atkins Museum of Art, Kansas City, Missouri). The motet form originates out of the Ars antiqua tradition of Western European music. Manuscript culture develops out of this time period in cities in Europe, which denotes a shift from monasteries to cities for books. Pecia system of copying books develops in Italian university-towns and was taken up by the University of Paris in the middle of the century. Wooden movable type printing invented by Chinese governmental minister Wang Zhen in 1298. The earliest known rockets, landmines, and handguns are made by the Chinese for use in warfare. The Chinese adopt the windmill from the Islamic world. Guan ware vase is made, Southern Song dynasty. It is now kept at Percival David Foundation of Chinese Art, London. 1250 – Cliff Palace, Mesa Verde, and other Ancestral Pueblo architectural complexes reach their apex[17] 1280s – Eyeglasses are invented in Venice, Italy. Late 13th century – Night Attack on the Sanjo Palace is made during the Kamakura period. It is now kept at Museum of Fine Arts, Boston. Late 13th century – Descent of the Amida Trinity, raigo triptych, is made, Kamakura period. It is now kept at the Art Institute of Chicago. The Neo-Aramaic languages begin to develop during the course of the century. Christianity in the 13th century ^ "Samudra Pasai worthy to be world historical site". Republika Online. 2017-03-24. Retrieved 2020-01-24. ^ Coedès, George (1968). Walter F. Vella (ed.). The Indianized States of Southeast Asia. trans.Susan Brown Cowing. University of Hawaii Press. ISBN 978-0-8248-0368-1. ^ "St. Thomas Aquinas". Catholic Encyclopedia. Retrieved 2023-12-09. ^ Brooks, Christopher (2020). Western Civilization: A Concise History. NSCC Libraries Pressbooks. ^ Lee, Kenneth B. (1997). Korea and East Asia: The Story of a Phoenix. Greenwood Publishing Group. ISBN 9780275958237. ^ "Greater London, Inner London Population & Density History". www.demographia.com. Retrieved 2023-02-10. Quoting from The London Encyclopedia, Ben Weinreb and Christopher Hibbert, ed., Macmillan, 2010, ISBN 1405049251 ^ Van Cleve, T. C. (1972). The Emperor Frederick II of Hohenstaufen: Immuntator Mundi. Oxford. p. 143. ISBN 0-198-22513-X. ^ Kantorowicz, Ernst (1937). Frederick the Second, 1194–1250. New York: Frederick Ungar. p. 228. ^ "Ken Angrok". Encyclopædia Britannica. Retrieved 25 July 2010. ^ Weinstein, Richard A.; Dumas, Ashley A. (2008). "The spread of shell-tempered ceramics along the northern coast of the Gulf of Mexico" (PDF). Southeastern Archaeology. 27 (2). Archived from the original (PDF) on 2012-04-25. ^ Grousset, Rene (1988), Empire of steppes, Wars in Japan, Indochina and Java, New Jersey: Rutgers University Press, p. 288, ISBN 0-8135-1304-9. ^ Kahler, H. (December 31, 1981). Modern Times. Brill Archive. ISBN 9004061967 – via Google Books. ^ "History of Aceh". Archived from the original on August 13, 2012. ^ Weatherford, Jack (2004). Genghis khan and the making of the modern world. New York: Random House. p. 239. ISBN 0-609-80964-4. ^ "Kenelle kellot soivat? – Kiipeä 360-videon avulla Turun tuomiokirkon torniin". Yle Uutiset (in Finnish). 2017-07-02. Retrieved 2023-02-10. ^ "Qutb Minar and its Monuments, Delhi". UNESCO World Heritage Centre. Retrieved 2023-02-10. ^ Berlo and Phillips, 275 James J. Walsh (1907). "The Thirteenth: Greatest of Centuries". nd.edu. Archived from the original on 2017-03-01. Retrieved from " 4 The following pages link to 13th century External tools (link count transclusion count sorted list) · See help page for transcluding these entries Showing 50 items. View (previous 50 | next 50) (20 | 50 | 100 | 250 | 500)Coin (links | edit) List of decades, centuries, and millennia (links | edit) Economy of Italy (links | edit) Imperialism (links | edit) Inca Empire (links | edit) Lavandula (links | edit) Levant (links | edit) Libro de los juegos (links | edit) History of Mali (links | edit) Romania (links | edit) Smelting (links | edit) 20th century (links | edit) 15th century (links | edit) 16th century (links | edit) 17th century (links | edit) 18th century (links | edit) 14th century (links | edit) 1st century (links | edit) 4th century (links | edit) 12th century (links | edit) 11th century (links | edit) 1282 (links | edit) 7th century (links | edit) 10th century (links | edit) 9th century (links | edit) 8th century (links | edit) 6th century (links | edit) 5th century (links | edit) 3rd century (links | edit) 2nd century (links | edit) 4th century BC (links | edit) 1st century BC (links | edit) 2nd century BC (links | edit) 3rd century BC (links | edit) 5th century BC (links | edit) 6th century BC (links | edit) 21st century BC (links | edit) 11th century BC (links | edit) 1299 (links | edit) 1326 (links | edit) 1359 (links | edit) 1389 (links | edit) 1154 (links | edit) 1163 (links | edit) 1160s (links | edit) 1380 (links | edit) 1141 (links | edit) 1135 (links | edit) 1204 (links | edit) 7th century BC (links | edit) View (previous 50 | next 50) (20 | 50 | 100 | 250 | 500) Retrieved from " WhatLinksHere/13th_century" Caller ID spoofing is a method scammers use to disguise their phone number and make it look like the call is coming from a trusted source. Whether it's pretending to be your bank, a government agency, or even your own number, these calls are designed to trick people into revealing personal information or transferring money. At DontSpoof, we have extensively studied how scammers use caller ID spoofing to deceive individuals. According to the Federal Communications Commission (FCC), billions of robocalls and spoofed calls are made every year, with many used to commit fraud. In this article, we'll explain how caller ID spoofing works, why attackers use it, and how you can identify these fake calls. Caller ID spoofing happens when a scammer manipulates the phone number information transmitted to your phone's caller ID to make it look like someone else is calling. This allows the scammer to impersonate a trusted individual or organization, making the call seem legitimate. The goal of caller ID spoofing is to trick victims into answering the call and believing the scammer's message. In some cases, the number displayed may be local or familiar to the victim, creating a sense of trust or urgency. Caller ID spoofing takes advantage of the way phone networks transmit information. Typically, when a call is made, the network sends the caller's phone number and possibly their name to your phone's display. However, this data can be manipulated, allowing scammers to change the number that appears on the recipient's caller ID. Here's how the process works step-by-step: Falsifying the Caller ID Information: Attackers use special software or services to change the phone number that appears on the recipient's screen. For example, they could make the call appear as if it's coming from a legitimate organization, such as a bank, utility company, or government agency. Example: A scammer calling from a number that appears as "IRS: (800) 555-1234" when in reality, the call is coming from an entirely different location. Creating a Sense of Urgency: Once the victim answers the call, scammers often use urgent language to scare the recipient into taking immediate action. They may claim the victim's bank account is compromised, or there's an urgent legal issue that needs to be resolved. Example: A caller claiming to be from your bank might say, "We've detected suspicious activity on your account. Please confirm your account details now, or we will have to freeze your account." Collecting Personal Information: The scammer then asks for sensitive data, such as your Social Security number, credit card details, or banking information, to "resolve" the fabricated issue. Example: A scammer pretending to be from Social Security might say, "Your Social Security number has been compromised. To verify your identity, please provide your number and additional details." According to Truecaller's 2023 Global Spam Report, over 68 million Americans fell victim to phone scams last year, many of which involved caller ID spoofing. Caller ID spoofing is an effective tool for scammers because it plays on trust. Here are the main reasons why they use this method: Increased Trust: Calls from local numbers or well-known organizations are more likely to be answered. In fact, according to First Orion, 94% of people are more likely to answer a call if the number is local or familiar. Example: A scammer may spoof a local area code to make you believe it's a neighbor or nearby business calling, such as (555) 123-4567, even though the real caller could be across the world. Bypassing Call Blocks: Many people rely on call-blocking apps or services to avoid unknown numbers. By spoofing a trusted number, scammers can bypass these filters and ensure the call gets through. Example: A spoofed call might appear as "John Smith (Your Neighbor)", even though the real caller ID is hidden or manipulated. Creating Urgency: Caller ID spoofing is often combined with urgent requests to pressure the victim into making hasty decisions, such as providing personal information or making payments. Example: A caller pretending to be from the IRS might say, "There is a warrant for your arrest due to unpaid taxes. You must pay immediately or face legal consequences." At DontSpoof, we have seen how these tactics are used in mass robocall campaigns to deceive thousands of victims daily. Here are two real-world examples showing how caller ID spoofing has been used in large-scale scams: One of the largest and most well-known caller ID spoofing scams involved scammers impersonating the IRS. The fraudsters spoofed the IRS's phone number and called victims, claiming they owed back taxes and would be arrested if they didn't pay immediately. Impact: The Treasury Inspector General for Tax Administration (TIGTA) reported that this scam affected over 1.8 million Americans and caused $72 million in financial losses . Victims were often tricked into sending money via wire transfers or prepaid debit cards. In another major scam, criminals spoofed the Social Security Administration's number, calling victims and telling them their Social Security number had been compromised. The scammers would ask for sensitive information under the guise of "verifying" the victim's identity. Impact: According to the Social Security Administration's Office of Inspector General, this scam resulted in more than $45 million in losses in 2021 . Victims were often elderly individuals who trusted the calls, believing they were speaking with legitimate government representatives. Despite their sophisticated appearance, spoofed calls often have subtle clues that can give them away. Here are some signs to look for: Unfamiliar Numbers Displaying as Local: If you receive a call from a local number that you don't recognize, be cautious. Scammers often use local numbers to increase the likelihood that you'll answer. Example: A number that looks like "(555) 123-4567" might appear local, but it's actually coming from a call center abroad. Your Own Number Appearing: Seeing your own phone number displayed on your caller ID is a telltale sign of caller ID spoofing. Scammers use this trick to bypass call filters and confuse the recipient. Example: If you receive a call from your own phone number or a number very similar to yours, it's a clear indicator of a spoofed call. Calls from Government or Financial Institutions: Be suspicious of unsolicited calls from agencies like the IRS, Social Security, or your bank. Legitimate institutions rarely, if ever, request sensitive information over the phone or demand immediate payments. High-Pressure Tactics: Scammers often create a sense of urgency, threatening legal action, account suspension, or arrest if you don't act quickly. This high-pressure approach is rarely used by legitimate companies. Example: A scammer might say, "If you don't provide your account information right now, your bank account will be frozen." At DontSpoof, we advise everyone to remain vigilant when receiving unexpected calls. If something feels off, trust your instincts and verify the caller's legitimacy through official channels. Caller ID spoofing remains a serious threat in today's world of phone scams. Scammers rely on this technique to disguise their identity, trick victims, and steal sensitive information. By understanding how caller ID spoofing works and learning the common signs of a spoofed call, you can protect yourself from falling victim to these deceptive tactics. At DontSpoof, we're committed to providing comprehensive insights into various spoofing methods, including caller ID spoofing, to help you stay informed and secure. For more details on different types of spoofing, explore our guide on Types of Spoofing. Have you ever received a call and seen a familiar number flash across your screen – maybe even your own? You answer, only to find it's a sales pitch, a suspicious offer, or even worse – someone trying to steal your information? Welcome to the world of Caller ID spoofing. It's a sneaky trick that bad actors use, and it's becoming increasingly common. Understanding how caller ID spoofing works and the caller ID spoofing threats it poses is the first step to protecting yourself. This isn't just a minor annoyance; it's a serious issue tied to phone scams that can have devastating consequences. We're here to break down the confusing world of fake caller ID and teach you how to protect against caller ID spoofing. Imagine someone trying to trick you by wearing a mask that looks like your friend's face. That's essentially what caller ID spoofing does with phone numbers. It's when someone deliberately changes the caller ID information displayed on your phone screen to disguise their real number. They're hiding their true identity and making it look like they are calling from a completely different number, and this is also the start of many robocalls and spoofing schemes. Think of it this way: your caller ID is like the return address on a letter. Normally, it tells you where the letter came from. But with spoofing, someone's deliberately putting the wrong return address on, making it seem like it came from somewhere or someone else entirely. Why do they do this? Well, the reasons are often far from innocent. Let's dive into the motivations and methods. Understanding the technical side of how caller ID spoofing works can be a bit tricky, but let's break it down: The Technology Behind It: Spoofing isn't some high-tech wizardry. It's relatively easy to do, especially with the help of technology like VoIP (Voice over Internet Protocol). VoIP lets you make phone calls over the internet instead of traditional phone lines. Many VoIP services have settings that allow users to change their caller ID information. This is where VoIP spoofing becomes a big problem. Spoofing Services & Software: There are also specific apps and services (some legitimate, some not so much) that make spoofing ridiculously simple. Some websites also offer spoofing services. They're often advertised for pranks or for business purposes, but they're easily misused. How the Phone System Is Tricked: When you make a phone call, your phone sends a signal to your network provider with your number. A spoofer, using those services, sends their call signal along with a fake caller ID number. Your phone provider then receives that signal and shows the spoofed number on the caller ID screen of the person receiving the call. It's like putting a fake address label on your package; the post office still delivers it, just to the wrong house. Now that we understand how it happens, let's talk about why it's a major problem. Caller ID spoofing threats are real, widespread, and can impact anyone. The consequences can range from simple annoyances to serious financial loss. The Rise of Phishing Calls: One of the biggest threats associated with caller ID spoofing is phishing calls. These are attempts to trick you into giving away personal information, like passwords, credit card numbers, or social security numbers. Spoofers often pretend to be someone trustworthy, like your bank, a government agency, or a tech support company. Because the number looks legit, you're much more likely to fall for the scam. Robocalls Become More Aggressive: Robocalls and spoofing go hand in hand. Spoofers use fake numbers to blast out massive amounts of calls, making it incredibly difficult to trace them. They know you are more likely to answer a local number or a number from your own area code, so they use fake caller ID to make you pick up. Increased Risk of Telecommunication Fraud: Telecommunication fraud, a type of crime involving fraudulent use of telecommunication systems, is often enabled by spoofing. Criminals can use spoofed numbers to commit identity theft, access your financial accounts, or even make unauthorized purchases in your name. It's not just about tricking you on the phone; it's about gaining access to your life. Financial Scams are Rampant: The core goal of many of these spoofing attacks is to get access to your money. They can use high-pressure tactics, scare you into sending money, or trick you into paying for "services" you don't need. The scam call identification becomes incredibly difficult due to the disguised caller ID information, which makes many people more vulnerable. To understand the real impact of caller ID spoofing, let's look at a few scenarios: The "IRS" Scam: You get a call from what appears to be the IRS. The caller ID matches a real IRS office. They claim you owe back taxes and threaten you with legal action if you don't pay immediately by wire transfer or gift card. This is a classic example of how spoofing creates a sense of legitimacy for a highly fraudulent scheme. The "Grandparent Scam": Imagine getting a call from a number that looks like it belongs to your grandchild. A panicked voice says they're in trouble and need money. You want to help, but the whole call is an elaborate setup using spoofing. The Tech Support Scam: A call comes in from what appears to be a well-known tech company. They claim your computer has a virus and you need to give them remote access to fix it, while they secretly install malware and steal your information. The fake caller ID makes it sound legitimate, when in fact it's a scam. "Neighborhood Spoofing": Ever answered a call only to be met by a recording and you notice that the call is from your area code and neighborhood exchange? Scammers use this tactic to make you think a neighbor is calling, increasing the likelihood you'll pick up. This is an aggressive tactic used in robocalls and spoofing to increase the percentage of people who answer the phone. These scenarios demonstrate how these seemingly simple tactics make it harder to exercise good judgment. Caller ID scams are designed to manipulate your trust. This makes cybersecurity and phone scams a serious concern for everyone. Okay, so it sounds scary. But the good news is there are steps you can take to protect yourself from becoming a victim of these phone scams and protect yourself against caller ID spoofing threats. Here are some practical tips: Be Skeptical of Unknown Numbers: The single best defense is to be suspicious. If you don't recognize the number, let it go to voicemail. If it's important, they will leave a message. Don't assume a number is legitimate just because it appears to be. Don't Trust Caller ID Alone: Remember, spoofers can make any number show up on your screen, even your own number. Never trust the caller ID information alone to determine the legitimacy of a caller. Never Share Personal Information: If a caller asks for personal information, like your social security number, bank account details, or passwords, hang up immediately. No legitimate organization will ask for that kind of information over the phone. Don't Give Into Pressure: Spoofers often use scare tactics to pressure you into acting fast. Don't let them rush you. Take a moment to think before acting and don't be afraid to hang up the phone. Verify Caller Identity: If you think the call might be legitimate, hang up and call back the organization using a number you find on their official website or statement. This ensures you are truly talking to the right entity. For example, if your bank calls and it seems unusual, find their customer service number online and call them to inquire. Utilize Call Blocking Features: Most smartphones offer call-blocking features. Take advantage of these to block suspicious numbers, and especially block numbers from areas you don't frequent or recognize. Report Suspicious Calls: If you think you received a spoofed call, report it to your phone provider and the FCC (Federal Communications Commission). This helps them track down these criminals and may be able to implement a solution to prevent further telecommunication fraud. Consider a Call Blocking App: Several third-party apps can help identify and block potential spam calls. They often use data from a network of users to detect likely robocalls and spoofing attempts. This can be a significant boost to caller ID spoofing prevention. Stay Informed: Keep up-to-date with the latest scams and trends. Criminals are constantly evolving their tactics, so the more informed you are, the better you can protect yourself. Be Aware of "One Ring" Scams: These scams involve letting the phone ring once and then hanging up. They want you to call back the number and usually they charge a large premium for the call. Do not call back any number you do not recognize. This is also another type of caller ID spoofing tactic. The good news is that authorities are cracking down on caller ID spoofing. The FCC has established rules and regulations to combat spoofing. Here's a quick overview: Truth in Caller ID Act: This act prohibits the use of spoofed caller ID for the purpose of defrauding or causing harm. However, the enforcement of this law can be challenging, as spoofers often operate from outside the US. STIR/SHAKEN Framework: The FCC implemented the STIR/SHAKEN framework. This technology helps to verify that caller ID is legitimate, reducing the effectiveness of spoofing. Although not a perfect solution, this framework is an important step in fighting back against fake caller ID. These efforts aim to create a system where it's harder to fake caller ID, but it doesn't remove the threat entirely. There's always going to be people and organizations actively trying to find new and different ways to make money from phone scams. Caller ID spoofing is a real and present danger, and it's constantly evolving. It's designed to take advantage of our trust and familiarity. By understanding how caller ID spoofing works, recognizing the caller ID spoofing threats, and taking the caller ID spoofing prevention steps outlined above, you can significantly reduce your risk of becoming a victim. Always stay skeptical, verify information, and be diligent in protecting your personal and financial information. The most effective tool against cybersecurity and phone scams is being informed and prepared. By staying aware, you can proactively guard yourself against these persistent attacks. Remember, protecting yourself from Caller ID scams is an ongoing effort, but it's an effort well worth making. Stay safe! Have you ever needed to send a call or a text, but preferred not to share your caller ID with the recipient? Caller ID spoofing can help you. Caller ID spoofing is a technology that allows you to send and receive phone calls or text messages from a caller ID that is different from your own. Caller ID spoofing services such as SpoofCard protect your caller ID when communicating with your smartphone, and give you the power to communicate anonymously when you otherwise could not. However, the technology that helps those looking for privacy and protection is also sometimes used by spammers and other bad actors. As a result, caller ID spoofing has received a bad reputation. Caller ID spoofing is the technology that allows you to alter the information forwarded to your caller ID in order to hide the true origin ID of the phone call. In simpler terms, caller ID spoofing allows you to display a phone number different than the actual number from which the call was placed. Caller ID spoofing technology works for both phone calls and text messages on your smartphone. Users can place calls from any caller ID they wish to display and can send and receive outgoing or incoming spoofed phone calls or texts from a phone number of their choosing or show their caller ID as "Unknown." The primary benefit of phone spoofing is the ability to stay anonymous so that you can get more accomplished and say what you need to when you otherwise might not be able or want to. Caller ID spoofing works in a few ways, the most popular being through VoIP (Voice-over-Internet-Protocol) technology. VoIP is the technology that allows for voice communications to be sent over an Internet connection rather than through a phone line or cell tower. Some VoIP providers allow users to configure the number they display as the caller ID through the configuration page on their website. In spoofing services which use VoIP, the process goes as follows: The user opens the application (web or mobile) of the spoofing provider. They enter the number they wish to call, followed by the number they wish to display. When they press "send" or "call," the call is sent through a VoIP service. The outbound caller ID is changed and the call is connected to the desired destination phone number. Using SpoofCard, you can spoof your caller ID for free on the SpoofCard website. To spoof your caller ID for free, follow the below steps: Download SpoofCard from the iOS or Android App Stores Sign up for free Enjoy the 5 free credits you get automatically just for signing up! After you've created your free account, you can use SpoofCard to make a call or send a text. Once you've used up your free credits, SpoofCard offers affordable credit-based plans to continue your spoofed calling. The easiest way to spoof your caller ID is with the SpoofCard app. SpoofCard allows you to easily spoof your caller ID for outgoing phone calls and text messages right on your smartphone. SpoofCard is just like having an unlimited amount of burner phone numbers right on your own smartphone! To spoof your caller ID when placing a phone call on your smartphone, follow these simple steps: Open the SpoofCard app Select "Make a Call" on the navigation bar Enter the phone number to call under "Number to Call" Enter the caller ID you wish to display under "Caller ID to display" Select voice changing, call recording, background noise, or straight to voicemail Select "Call" to place your spoofed call SpoofCard allows you to spoof your text messages just like you can spoof your phone calls. With SpoofCard, you can anonymously make it seem like you texted from a totally different number. The person you are texting will never know! All text message conversations remain within the SpoofCard app and function just like iMessage or Android texting. Best of all, you will see the replies and be able to continue the conversation through your spoofed phone number. Follow these simple steps to send a spoofed text message: Open the SpoofCard App Select "SpoofText" on the navigation bar Select "New SpoofText" Enter the phone number to send the text to, or select from your contacts Select the phone number you'd like to display as your Caller ID The short answer is yes, caller ID spoofing is legal, unless the spoofed call or text is sent with the intention to cause harm in some form. If no harm is intended or caused, spoofing is legal. In the United States, "Under the Truth in Calling Act," FCC rules prohibit any person or entity from transmitting misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value. Anyone who is illegally spoofing can face penalties of up to $10,000 for each violation. In some cases, spoofing can be permitted by courts for people who have legitimate reasons to hide their information, such as law enforcement agencies working on cases, victims of domestic abuse or doctors who wish to discuss private medical matters. The details regarding the legality and legitimacy of caller ID spoofing are not very well known, thanks to the scammers and telemarketers that use neighbor spoofing for their phone scams. Due to the recent publicity of the FCC's decision to allow phone service carriers to block caller ID spoofed calls, the stigma around caller ID spoofing is that all forms are harmful and illegal. As outlined above, this is simply not the case. In most cases, caller ID spoofing cannot be traced. Only in extreme circumstances can law enforcement agencies trace the origin of the spoofed phone call. This is done by using technology to determine what service was used to carry out the spoofing and subpoena that service to provide information and call records on the person in question. If you are looking to place a spoofed phone call or text message, it is unlikely that your spoofed caller ID will be traced back to your real phone number – unless you are spoofing your phone number with the intent to cause harm or damage. Despite the long list of ethical benefits caller ID spoofing provides, the unfortunate reality is that it is also used by bad actors and scam artists. Scammers employ a tactic called "neighbor spoofing" as their strategy to send harmful phone scams to unsuspecting victims, with the intent to steal their money or personal identity. Neighbor spoofing works by tricking recipients into thinking they are receiving a legitimate phone call by showing caller ID that matches or is close to your phone number's NPA-NXX. By matching their NPA-NXX closely to yours, spammers try to trick people into thinking the call is coming from a legitimate phone number because it looks as though it's coming from a phone number in your area code. This makes you far more likely to answer the phone and potentially fall for their elaborate phone scam. It is important to note, however, that though it is true caller ID spoofing has been used as a vehicle for scammers to complete their phone scams, is not entirely to blame for the growing epidemic of robocalls and phone scams. Like many tools or products that have been used to cause damage or harm to others, the people behind the phone scams are the root cause of the spam call epidemic. Though caller ID spoofing services such as SpoofCard have put intense measures in place to ensure their services do not fall into the wrong hands, phone scammers who are technologically adept can spoof their caller ID without using a service, as they have figured out ways to do it on their own. To truly stop harmful caller ID spoofing, we must address the root cause of the problem: the scammers behind the phone calls. Now that we've gotten past the elephant in the room, we can address the benefits and numerous uses that legal caller ID spoofing provides to individuals and professionals worldwide. The primary benefit caller ID spoofing provides is that it allows its users to maintain their anonymity while communicating over the phone – ultimately to protect one's own privacy. Below are a few real-world examples of how caller ID spoofing can provide value to its users. Doctors and veterinarians. Doctors and veterinarians value their privacy and prefer that their patients don't have their personal contact information, for understandable reasons. Due to those reasons, spoofing services are greatly valued to these people, who can still call patients from their personal cell phones or landlines after hours, all while displaying the caller ID information of their office. In addition, the call recording features found on spoofing applications, such as SpoofCard, are used to record conversations for notes and further analysis. Law enforcement officials and private investigators. Professionals who are tasked with finding suspects, persons of interest, or missing persons, frequently use caller ID spoofing to locate these people. Call spoofing can be used by professionals in order to appear as though they are calling these people from the numbers of their friends and family – it's easy to ignore a call from an unknown caller ID, but anyone will answer a call from their mother or their best friend. And when they answer those calls, separate services provide their location. In these instances, caller ID spoofing makes the job of an investigator much easier. Secret shoppers. For most mystery shoppers, one of their primary tasks is to conduct call center evaluations. This involves calling the customer support branch of a company with a particular set of questions and evaluating the expertise of the customer support representatives. These calls are generally recorded and call recording is a feature found in a number of call spoofing applications, namely, SpoofCard. Mystery shoppers can't make these calls using their actual number, so they use call spoofing applications to hide their number and to record the call to be sent to their superiors for evaluation. Personal Relationship Conflict Management. In a more personal example, caller ID spoofing can be used to manage relationship conflicts. Caller ID spoofing is a great tool to get people you need to speak to, to answer their phone calls or text messages when they otherwise might not. By changing your caller ID, you can speak to loved ones or friends who might be avoiding you or have even blocked your phone number. With caller ID spoofing, you can finally say what you need to – without the worry of your caller ID interfering. To summarize, the reality is that many times legal caller ID spoofing provides a great deal of value for those looking to use caller ID spoofing for the right reasons. Spoofing allows you to take full control over your caller ID so that you can get more accomplished, and it allows you to say what you need to when you otherwise could not. If you are looking for the best app to place spoofed calls and texts, look no further than SpoofCard. SpoofCard has helped over five million users protect their caller id and stay anonymous over the phone. With a 4.6 star rating and over 17,000 reviews, Spoofcard is the #1 rated service to send and receive spoofed calls and texts on Apple, Android, and your computer. Start protecting your phone number today! For Who?Cybersecurity professionals, IT managers, business owners, and fraud prevention teams looking to understand and mitigate the risks of Caller ID spoofing. It is also valuable for individuals concerned about phone security threats. Estimated Reading Time:8-10 minutes Reading Difficulty Level:Intermediate to Advanced – Designed for readers with a foundational understanding of cybersecurity, with technical details explained for broader accessibility. In today's hyper-connected world, cyber threats are no longer confined to phishing emails or malware-infected links. They're increasingly coming through one of our oldest, most trusted communication channels—the phone. Caller ID spoofing has evolved into a sophisticated method used by cybercriminals, exploiting phone networks to deceive individuals and businesses alike. For cybersecurity professionals and organizations alike, caller ID spoofing presents a unique challenge. Here, we'll explore caller ID spoofing in detail, examine its risks to businesses, and outline comprehensive strategies for preventing it. What is Caller ID Spoofing? Caller ID spoofing is the act of falsifying the caller's number displayed on the recipient's caller ID, making it appear as though the call is from a legitimate source. Cybercriminals manipulate caller ID information, often appearing as someone you trust, like a bank, government agency, or familiar business. This deception lowers the defenses of even the most cybersecurity-conscious individuals and enterprises, making them more vulnerable to information theft, fraud, and unauthorized access. How Caller ID Spoofing Works: The Technical Side The technology underlying phone systems was not initially designed with security in mind, particularly around verifying the caller's identity. Spoofing exploits this vulnerability by using Voice over IP (VoIP) services, call-modification software, or third-party spoofing services to alter the caller ID that appears to the recipient. This technology enables attackers to pose as a trusted contact or familiar entity, creating a false sense of security that leads to devastating consequences. Common Tactics and Threats in Caller ID Spoofing Business Impersonation Scams: Cybercriminals impersonate legitimate businesses to extract sensitive information from unsuspecting employees or customers. Spoofed calls often mimic help desks, IT support, or executive requests, tricking recipients into providing credentials, sensitive data, or even transferring funds. Supply Chain and Vendor Fraud: In increasingly digitized supply chains, fraudsters may pose as trusted suppliers, requesting urgent payments or information that can lead to financial loss and data exposure. Spoofed numbers can match those of actual vendors, making detection challenging without stringent verification processes. Account Compromise and Phishing: Through social engineering, attackers use spoofed calls to gather enough information to compromise accounts. For instance, they might pose as an HR representative or IT department, asking for login details or personal identifiers that provide access to sensitive systems or data. Government and Law Enforcement Impersonation: By pretending to be government or law enforcement officials, scammers intimidate recipients into sharing information, making payments, or even granting remote access to their devices. This tactic is particularly effective against smaller businesses or less security-mature individuals within an organization. Executive or "CEO Fraud": In this scam, the attacker impersonates a high-ranking executive, asking employees to conduct urgent and confidential transactions. These spoofed calls may instruct employees to bypass standard processes, making them harder to track and prevent without prior training on such tactics. Risks of Caller ID Spoofing for Businesses Caller ID spoofing can lead to multiple issues, many of which have ripple effects across an organization: Financial Loss: Attackers often deceive employees into approving transactions or revealing sensitive payment information, resulting in significant monetary losses. Data Exposure: Spoofed calls can trick employees into disclosing confidential company or customer data, leading to severe privacy violations and reputational damage. Network and System Breaches: Through social engineering, attackers may gather login credentials or other information that allows unauthorized access to systems. Reputational Harm: Customers or partners who fall victim to spoofing impersonations may lose trust in your brand, damaging relationships and future business. Operational Disruption: Repeated fraudulent calls can disrupt business operations, diverting attention and resources to managing and mitigating these threats. Comprehensive Strategies to Combat Caller ID Spoofing Implement Multi-Layered Verification Processes: For sensitive requests—especially those involving financial transactions or confidential information—establish multi-step verification procedures. Require verification through a different communication channel or an internal system that can confirm the request's legitimacy. Adopt Caller Authentication Technology: The STIR/SHAKEN framework, which is now widely deployed in the United States, authenticates the caller's number to reduce the likelihood of spoofed calls. While not foolproof, it provides an added layer of verification, particularly for businesses working with telecom providers that support the technology. Train Employees on Caller ID Spoofing: Educate your team on the risks of spoofing, emphasizing the need to verify all unusual or sensitive requests. Ensure that they know the common signs of spoofing, such as a sense of urgency, unusual requests, or caller hesitation. Regular training and simulated social engineering exercises can enhance employee resilience to these tactics. Integrate Anti-Spoofing Solutions and Security Controls: Many cybersecurity platforms offer anti-spoofing technology that can filter out suspicious calls or flag high-risk numbers. These solutions can integrate with broader threat detection systems to monitor and block phishing attempts across phone, email, and messaging channels. Encourage a Culture of Caution: Foster an environment where employees feel empowered to question and validate requests, even from high-ranking officials or familiar contacts. This culture can significantly reduce the risk of social engineering and insider attacks. Use Call-Blocking and Reporting Tools: Certain telecom providers offer call-blocking services specifically designed to combat spoofing. Encourage your team to report suspicious calls to telecom providers and regulatory bodies, helping these organizations track and address fraudulent patterns. Set Up and Enforce Strong Internal Policies: Develop clear guidelines for handling phone-based requests for information, payments, or access. For example, you can implement policies that mandate cross-channel verification for sensitive actions and specify sanctions for unauthorized deviations from these policies. How the Industry is Fighting Caller ID Spoofing Telecom providers and regulatory authorities worldwide are stepping up efforts to reduce caller ID spoofing, but the fight requires ongoing vigilance. The Federal Communications Commission (FCC) in the U.S., for instance, has implemented requirements for telecom providers to authenticate calls using the STIR/SHAKEN framework, which validates the origin of each call. While these solutions don't fully eliminate spoofing, they have helped mitigate some of the risks, especially for those who adopt additional anti-spoofing measures. Final Thoughts: The Need for Vigilance and Education Caller ID spoofing is a growing threat that impacts individuals and businesses alike, posing risks that extend far beyond financial loss. For organizations, combating caller ID spoofing isn't solely about technology; it's also about awareness, training, and a proactive approach to verifying calls. Employees should be empowered to question suspicious requests, and businesses must adopt a multi-layered strategy to ensure their defenses against this invisible threat remain robust. In the realm of cybersecurity, vigilance is critical. Staying informed about tactics like caller ID spoofing and taking preventative measures can mean the difference between a secure organization and one that falls victim to cybercriminals. Educating your workforce, leveraging advanced anti-spoofing technology,

and fostering a culture of caution will help safeguard against the hidden dangers of caller ID spoofing, ensuring your business remains resilient in the face of evolving threats. Call spoofing has enabled people to fake the return number that is shown by Caller IDs for many years now, and the ability to “spoof” a phone number has become widespread. Spoofing, in simple terms, just means that the number shown on someone’s caller ID is not the actual number that is placing the call. As opposed to a fake number, spoofing a number lets callers appear to be a number more familiar with the recipient.People spoof caller ID numbers for a wide variety of reasons.They perform a classic prank call to their neighbor or friend.They protect their privacy and phone information from being captured and sold to third parties.They want a secondary number captured by recipients.They want to reserve their actual phone number for their close family and friends while using a secondary number for “social media” friends and other parties.They call a debt collector with a spoofed number to avoid repeated calls in the future.They investigate a number they are curious about.They attempt to confirm or investigate a “potential” scam call.They use it to actually scam others by faking the number so the recipient thinks it is someone local, or a person or business they know.With more and more people starting to ignore calls from unfamiliar numbers and sending them to voicemail automatically, it has made pulling off a classic prank call trickier. However, spoofing a number that the victim recognizes, has become a popular scenario for scam artists and pranksters alike.In 2020, it’s more important than ever to practice safety when it comes to your personal identification. While it may be difficult to change your phone number on all services or registrations to a spoofed number, you can still protect your identity by making sure that your new number spreads to as many services as possible. This way, you will receive return calls on a number that can be easily disposed of if anything were ever to go wrong with the intended caller.Yes. At its core, there’s nothing illegal about the act of spoofing caller ID with a false number in the United States. It is your intentions that generally determine the legality of your actions.If you hide your real number to contact a business to protect your personal information, it’s legal.If you fake your phone number to investigate a potentially risky call, it is legal.If you get a second phone number for specific contacts, it is legal.If you hide your real number to prank a caller, it is often legal, but your actions may be considered illegal depending on location and circumstances. It can be an act of falsifying information in an attempt to harass or abuse, etc.If you spoof your phone number to scam the recipient, it is questionably legal, but your intentions and actions are definitely illegal!If you call from a disposable number to threaten the recipient, it is possibly illegal due to your intentions and the falsification of caller identity (trickery). However, the action of threatening the recipient is definitely illegal.For legitimate, non-criminal motivations, you are in the clear. So using a spoofed number to trick your friend into thinking that the President is calling him on his birthday may be more or less funny depending on your sense of humor, but it is legal. The official word from the FCC websiteIf you spoof your number to trick him into thinking he’s talking to his credit card company, and you attempt to get his card details, it is a crime.There are basically three different ways to spoof a number or call.You can register for a permanent number through a call forwarding website or app.You can get a temporary number from sites more oriented towards “burner” numbers.You can use various apps to enter a false phone number that displays on the recipient’s caller ID, while actually just using your own number to make the call.You can’t personally stop the identity leaks from happening, but by using a spoofed number, you can make the fallout a little less catastrophic. Spoofed numbers can come in two different varieties, depending on what you’re looking for. Permanent numbers don’t change or recycle and can be held by you for as long as you’ll need them. In fact, they’re a real number, just connected to a phone you don’t answer if they’re connected to a phone at all. Disposable numbers, on the other hand, are designed to be cycled through, used for a certain duration before being tossed in the trash. Whether or not that’s something you’re looking to use is up to you, and really, the type of number you’ll be using really depends on the scenario you find yourself in. Still, we’ll cover both options below, with some great suggestions for both free and paid spoof numbers.While you still have to dedicate some time to managing your fake number, as you would your real number, you’re secure if your false number ever leaks online. These permanent services usually offer some amount of call blocking and restricting features. Being able to ensure your number is always in your grasp means that you can place your false number on more important documents, giving it out to your dentist or doctor for appointments, or placing it on job applications to protect your standard account service. Permanent number services are also typically cheaper than their temporary counterparts, as you’ll discover in the next segment.The first service you should take a look at for a secondary spoof number is, unsurprisingly, Google Voice. Voice is for someone looking for a secondary, web-based number that doesn’t cost anything. Google offers a desktop and mobile web client, along with dedicated clients for both iOS and Android that are sleek and regularly updated. Google Voice allows you to use your assigned secondary number to forward calls to your primary number, all while making free phone calls throughout the United States. Your assigned number is able to be customized as well, so you can select a specific area code throughout the US, or type the last-four digits to make it easy to remember.Like Google Voice, Talkatone is built around providing alternate numbers to call and text US-based users for free (and to call and text numbers outside the United States for small charges). Talkatone even lets you change this number when you need to. This makes the service bit less permanent while simultaneously giving you more flexibility should your number get leaked online. The downside to Talkatone is ads within the app. Textfree has been around for nearly a decade, and you can still grab a free number through their service by signing up through the website or mobile application. You can choose your area code and memorable number patterns when signing up for a number. You can keep the number as long as you want, though you’ll need to use it once every 30 days to place a call.There are also paid, premium options available, including Flyp, Hushed, TextNow, and Sideline.Sometimes, you just need a number for one-time use or for a certain period. Disposable numbers are great. You can call a business or an individual, hang up the phone following your conversation, and toss the number away, leaving the person without a way to contact you again. Unfortunately, disposable numbers rarely come without a fee attached.Burner is an app that automatically gives you a new number whenever you need one. Your number is real and can be used to call and text from within the app, and the caller ID displays your Burner info instead of your actual phone number. The app is smooth and responsive, and you get a free number for seven days upon installation. Depending on how many numbers you need and how much you’ll be using the app, Burner can get really expensive, really fast.Flyp offers support for multiple secondary numbers, making it easier to cycle through plans. Of course, paying the monthly fees can get expensive rather quickly. If you plan on holding multiple numbers at once, this spook call service might get costly. Still, the ability to mirror local area codes while placing a call is ideal for someone looking to spoof numbers with only one account, and with great audio quality.Hushed offers both permanent and disposable numbers. The app provides the ability to dispose of numbers at any time, so long as you’re paying for the service. Hushed stands out with its end-to-end encryption when talking to other users. This makes the service the most secure phone number app on the list, and that may be important if you’re trying to hide your identity. All numbers are disposable. There’s no credit card needed to sign up for an account, and calls can be sent and received from anywhere. Hushed is also one of the more affordable paid plans.There are a number of services online that provide spoofed calling numbers on a one-shot basis. That is, after you’ve registered at the site and paid the subscription fee, you can enter the number you want to call and the number that you want to appear on Caller ID. The call will go through on your smartphone or landline, or via your web browser. You can use as many different numbers as you wish and can assign a new number for every call you make if you want.SpoofCard is reputable, and they are one of the oldest spoofing providers in the industry. SpoofCard offers a number of features, including the ability to artificially disguise your voice and even change its gender presentation. The service also provides the ability to record calls for later playback (priceless if you’re planning on pranking your friends), the addition of background noises like traffic, a nightclub, or police activity for added realism, and the ability to send calls directly to voicemail. You can also dial multiple recipients at once, or add more people on your end of the call to listen in. SpoofCard also allows you to send spoofed SMS text messages. The service is definitely optimized for pranksters.SpoofCard offers a 60-second free trial, offers a web version, as well as an Android app and an iOS app. Charges are based on bulk minute packages, paid as a one-off purchase, or as a monthly subscription. SpoofCard supports calls to non-US destinations but uses more credits per minute.SpoofTel is another service providing instant spoofing service on-demand. SpoofTel offers a desktop app for Windows and an iOS app. The iOS version requires a jailbroken phone. SpoofTel has the ability to change your voice pitch and add soundboard audio to the background. SpoofTel offers SMS text message spoofing as well. Costs are based on a per-minute basis, in addition to added features like voice changing and recording.Spoof Call does not offer app versions; all calls occur via the service’s website. The service has some unique features, including call recording, voice changing software, limited background noises, group calls, and a text-to-speech converter with multiple language choices. Spoof Call is based in Europe, but the credits they sell are valid for US calls (among other locations).Since 2015, a group of telecom engineers from major carriers started developing a way to stop call spoofing in its tracks. In recent years, spoofing has gone mainstream. The widespread nature of call spoofing has begun to undermine public trust in the integrity of the phone system. The engineering teams are relying on two new systems to stop it: STIR (Secure Telephone Identity Revisited) and SHAKEN (Signature-based Handling of Asserted information using tokens).The idea behind STIR and SHAKEN is to give every phone a certificate of authenticity, a digital signature, that becomes the sole source of caller ID information. Caller ID would become trustworthy once more. The basic idea is ridiculously complicated, but here is a simplified explanation. A person places a call. That call’s data stream would contain the certificate (in digital form) that verified that the call was coming from the number it claims to be coming from. As the phone call passes through the circuitry, the carrier would check the validity of the certificate using a public/private key system. A call whose certificate failed to pass validity would either get blocked or display a warning message in the caller ID field.FCC mandates that all voice carriers effectively implement STIR/SHAKEN authentication by June 30, 2021.There are other resources available at TechJunkie to help you combat call spoofing efforts.Is there a way to tell if a spoofed number is calling?It’s highly improbable that you’ll know a number is spoofed until you answer the phone call. If someone is spoofing a number that you’re familiar with, you probably won’t know that’s what’s happening until you pick up the call.If the number calling is unfamiliar to you but spoofed using the same area code as your phone number, you can do a reverse lookup on the phone number. If the number is spoofed, the search results will turn up no information. Also, calling a spoofed number back will likely result in a busy signal rather than actually getting to talk to someone.How do I avoid being scammed?Spoofed numbers can be incredibly tricky, it gives any scammers the upper-hand. If you receive a phone call from a company asking for any personal information, it’s best to hang up and call the company from a phone number that you’re familiar with. AT&T for example had an issue with their customer service number being spoofed. The scammers would offer bill credits but they’d need the account Passcode to access the account. Most reputable companies will never ask you for any information if they call you. The FCC warns that scams resulting from spoofed numbers usually happen after a natural disaster, or to gain access to your credit information. Caller ID spoofing has long been the domain of pranksters and scammers, but although the technology often is used unethically, there may be a few legitimate reasons why you would want to disguise your phone number's Caller ID, rather than just block it. Here are a few that come to mind and easy ways to masquerade as someone else. Some Non-Evil Uses for Caller ID SpoofingThanks to the Caller ID Act of 2009, using Caller ID spoofing for causing harm or defrauding someone is a crime. (Telemarketers are also required by the FCC to use an accurate Caller ID number when they call you.)Caller ID spoofing in general, however, isn't illegal in the US. There are at least three scenarios where you might want to use it:Perhaps you're working from home one day but need to place a call to a client or customer and want to appear to be working from the office—or just not give out your home or cell number (Doctors in particular may have this need). With Caller ID spoofing, you can appear to be placing the call from your office.Another case scenario is if your friend is ignoring your calls or is simply notoriously hard to get a hold of on the phone, and you really, really need to get through. You should only use Caller ID spoofing in an emergency case, because once your friend answers and finds out you spoofed the Caller ID, it had better be worth it.Caller ID spoofing is also great for surprising young children: You can place a call as Santa or Cinderella or whoever (many services and apps disguise your voice). This might only work with really young children, however, especially with the limited choices you get for voice disguises.How to Spoof Your Caller IDBetween 2004 and today, dozens and dozens of Caller ID spoofing companies have been established to meet this incredible need for people to spoof their phone numbers.SpoofCard is one of the biggest and oldest, and it offers a free test drive of its service. Enter your number, the number you want to call, and the number you want to be displayed on their website widget to place the call. This is the service I used to place a call supposedly from 867-5309, you know, from Jenny in that song (SpoofCard unfortunately doesn't let you enter in a Caller ID name). SpoofCard and other services like it work like a calling card, if you've ever used one of those. You dial a number provided to you by the service and then enter an access code or PIN number, plus the recipient's number and your fake caller ID. Also like phone calling cards, you buy credits, starting at $4.95 for 25 credits (1 minute per credit).Spoofingcards.com has a table comparing SpoofCard with Bluff My Call and Stealth Card, two other services in this space. There are several other providers, and they all seem to work pretty similarly, many with mobile apps so you can spoof away from your cell phone.My advice, if you're going to do this, is to try out the service first if it offers a free call. I tried out SpoofTel, which offers a free trial and also lets you enter in a display name to be shown in Caller ID, but the call came in as "Unknown" to my phone, which pretty much defeated the purpose. Good thing it wasn't a really critical call I needed to get through to myself.Lifehacker's Evil Week is all about topics such as password cracking, social hacking and other questionable tricks to make sure you're in the know. Knowledge is power, and whether you use that power for good or evil is in your hands. You can follow or contact Melanie Pinola, the author of this post, on Twitter or Google+. Your caller identification display (Caller ID) normally indicates the phone number and name associated with the line used to call you. Caller ID spoofing is the act of altering the Caller ID displayed to the person receiving the call. Caller ID spoofing can be used for legitimate and illegitimate purposes. Examples of legitimate use of Caller ID spoofing A call centre that places legitimate calls on behalf of clients and alters its Called ID information to display its client’s name and telephone number. A doctor calling to discuss a patient’s lab results may want to display the hospital’s general call back number as their Called ID to direct all future inquiries appropriately. Examples of illegitimate uses of Caller ID spoofing Illegitimate telemarketers that change their Caller ID information to misrepresent themselves and to trick Canadians into answering the call. The Caller ID is altered to match the first 6-digits of your telephone number so that it looks like a local call, perhaps even from a neighbour in your area. This practice is often referred to as “neighbouring“. The Caller ID is altered to display your own telephone number. This practice is often referred to as “mirroring“. The Caller ID is altered to display the number of another individual and/or organization (i.e., pose as a recognizable brand or a government organization). Is Caller ID spoofing illegal? Telemarketers who make calls to Canadians are required to accurately identify themselves and their client. However, when telemarketers use technology to spoof their Caller ID to display inaccurate, false or misleading information, they are in direct violation of this requirement. As a result, each violation of the Unsolicited Telecommunications Rules can lead to fines of up to $1,500 per violation for an individual and up to $15,000 per violation for a corporation. How do I protect myself from spoofed calls? Register your telephone number on the National Do Not Call List File a complaint about an unwanted telemarketing call Note: If you suspect fraud, you can report it to your local police force or the Canadian Anti-Fraud Centre (1-888-495-8501), a national service jointly operated by the Royal Canadian Mounted Police, the Ontario Provincial Police and the Competition Bureau. Check out our Telemarketing Consumer Alerts page to help you identify common problematic telemarketing campaigns that use Caller ID spoofing. Be cautious if you are asked to provide personal information (e.g., banking information, passwords). When in doubt, hang up and call the number on your bank statement or the organization’s website. Certain calling features may be available to you to block or filter unwanted and illegitimate telemarketing calls. Phone service providers and other parties have to provide information on the calling options and features available to help Canadians protect themselves from these calls. Read the Summary of Options Currently Available to Canadians to Manage Unwanted Calls. What else is the CRTC doing about it? Following a public consultation, we have issued a notice of consultation to better protect Canadians against unwanted and nuisance calls. The following measures are being implemented by phone service providers. Traceback process At our request, a telecommunications industry working group developed and deployed a call traceback process. The objective is to identify the origin of unwanted calls on the Canadian network, regardless of the type of technology used by the caller. The end goal is to enforce the Unsolicited Telecommunications Rules by enabling corrective action to be taken at, or close to, the source of such calls. Caller ID authentication and verification measure We directed telecommunications service providers to implement a framework to authenticate and verify caller identification information for Internet Protocol (IP)-based calls. This framework is called STIR/SHAKEN, which stands for Secure Telephony Identity Revisited/Signature-based Handling of Asserted information using toKENs. The STIR/SHAKEN framework enables service providers to certify whether a caller’s identity can be trusted by authenticating and verifying the caller ID information for IP-based voice calls. This framework empowers Canadians to determine which calls are authenticated, reducing the frequency and impact of caller ID spoofing. Presently, not all calls received will be authenticated due to a variety of reasons such as: network compatibility calls being not entirely performed over an IP-voice network complex call scenarios and the fact that only smartphones are able to display the STIR/SHAKEN information More Canadians will be able to see the effect of the STIR/SHAKEN framework as service providers continue to: upgrade their network to IP technology, make compatible phones available to their customers improve their capacity to properly authenticate caller IDs We expect STIR/SHAKEN, to partner with the analytical capacity of service providers to effectively protect Canadian consumers against fraudulent automated call systems and other similar nuisance calls. Universal Call Blocking and Call Filtering Phone service providers that are not already offering an opt-in call filtering system are required to block all calls with caller IDs that: exceed 15 digits, or are not dialable according to the North American Numbering Plan (For example, calls from the number “999-999-9999” would be blocked before reaching the subscriber). The call filtering option, which can be offered as an alternative, should be able to detect suspicious calls and intercept them (either by sending them directly to voicemail or requesting the caller to provide an input on their phone keypad to reach the customer). Industry Initiative On December 9, 2021, we approved Bell Canada’s application to deploy its new call-blocking technology. The call-blocking system leverages artificial intelligence to analyze telecommunications traffic to flag anomalies that suggest possible fraudulent activity at the network level. The approval is a direct result of a successful trial period, during which more than 1 billion fraudulent calls were blocked. Date modified: 2023-05-25 Over the years, law enforcement officials and collection agencies have utilized caller ID spoofing to mask their actual numbers. These entities used it to increase the likelihood of their calls being answered. It laid the groundwork for what was to come. In 2004, a historic moment occurred with the launch of Star38.com, the first service specifically designed to offer caller ID spoofing for the general public. Soon after, similar services skyrocketed, dramatically increasing the ease of executing spoof calls. Accessibility to spoof calling led to a spike in scams, particularly noted in online marketplaces like eBay and Craigslist. Fraudsters often pose as buyers from reputable locations to gain sellers’ trust and personal information and then use it for fake sale schemes. One of the most significant impacts of caller ID spoofing was seen in the 2015 IRS scam when scammers spoofed the IRS’s phone number to call thousands of Americans. They claimed they owed back taxes and demanded immediate payment. The 2015 IRS scam highlighted the growing issue of caller ID spoofing and its potential for significant harm. With technology advancements, Caller ID Authentication and spam detection apps have emerged to combat scam calls, yet caller ID spoofing remains a challenging issue. Like Spoofbox and get free credits every day! Share — copy and redistribute the material in any medium or format for any purpose, even commercially. Adapt — remix, transform, and build upon the material for any purpose, even commercially. The licensor cannot revoke these freedoms as long as you follow the license terms. Attribution — You must give appropriate credit , provide a link to the license, and indicate if changes were made . You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use. ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original. No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits. You do not have to comply with the license for elements of the material in the public domain or where your use is permitted by an applicable exception or limitation . No warranties are given. The license may not give you all of the permissions necessary for your intended use. For example, other rights such as publicity, privacy, or moral rights may limit how you use the material. What is caller ID spoofing? Caller ID spoofing is when someone intentionally alters the information relayed to your caller ID display to hide their identity or impersonate somebody else. Imagine you're going about your day when your phone begins to ring, with your phone's caller ID indicating that the call is coming from your bank. Upon answering the phone, a voice on the other end informs you that someone has hacked the password to your online banking account and that you need to provide your personal information to verify your identity and secure your account. After following their instructions, you hang up and rush to your computer. You then discover that your account appears to be perfectly fine. As you go to call them back, you realize the number that called you doesn’t match the number listed on your bank's website. This is possible due to caller ID spoofing, a technique used by scammers to impersonate others or disguise their own identity. To learn more about caller ID spoofing and how to spot and avoid spoofed calls, read through this helpful guide. How caller ID spoofing works: 3 techniques to know With the help of caller ID spoofing, con artists can place phone calls that appear as if they are coming from somebody else. This type of phone spoofing can be implemented in different ways and may be used for vishing or other scams. To help you better understand how caller ID spoofing works, let’s explore some common spoof call methods. VoIP spoofing When scammers first began practicing caller ID spoofing, it required advanced technical knowledge and expensive equipment to pull off. Thanks to Voice over Internet Protocol (VoIP) technology, caller ID spoofing can be done for little to no cost without specialized equipment. VoIP is a calling service that allows users to place calls over the internet. While this may be a great alternative to traditional calling services, it can also be used for caller ID spoofing. This is because scammers can customize their caller ID display name when setting up their accounts, allowing them to easily impersonate someone else. In addition, VoIP services aren’t subject to the same hardware standards as landlines, which makes VoIP caller ID spoofing much easier than doing it through a traditional landline. Because VoIP is often cheaper and easier to set up than a landline, a scammer may use it to carry out scams, such as IRS scam calls, which is when a scammer impersonates the IRS to steal your personal information. Spoofing services As the name suggests, spoofing services are services designed specifically to help users spoof a call. In some cases, these services are web-based platforms or third-party apps. With these services, scammers can easily customize their caller ID information either for a small fee or at no cost at all. Because this can be as simple as downloading a free app, using a phone spoofing service can make phone number spoofing easy and accessible for scammers of all skill levels. In addition, these services can also be used to send text messages and may be used for smishing attacks. Orange boxing Orange boxing is an alternative method of call spoofing used to trick someone into thinking that they are receiving a call from a spoofed number when there is actually no phone call at all. This is possible using hardware or software that can mimic the signal of an incoming call, allowing the scammer to spoof the caller ID display. Because this method of caller ID spoofing doesn’t spoof a legitimate phone call, it is often used as a social engineering technique to scare you or make you believe that someone else is trying to contact you. How to spot caller ID spoofing: 5 red flags With an understanding of how caller ID spoofing works, you may wonder how to spot a spoofed call. After all, the point of caller ID spoofing is to trick you into thinking you’re talking to someone else. With that in mind, there are still some red flags you can watch out for whenever you receive an incoming call, including: Unfamiliar number: If you recognize the caller ID display name but not the associated phone number, it may be a spoofed call. Pre-recorded messages: In some cases, caller ID spoofing may be used for robocalls. In these calls, you may be asked yes or no questions or to press a specific number for further instructions. As with all unknown callers, it's best to treat these as spam and hang up immediately. Sense of urgency: Another sign of spoofed phone calls is a sense of urgency. For example, a scammer may use caller ID spoofing to pose as a friend in danger. In this type of scam, the scammer may inform you that they are in a desperate situation and need money as soon as possible. Scammers will do this to scare you and get you to act quickly without confirming that the call is from who they say they are. Requests for payment or personal information: Whether you’re greeted by a recording or a live caller, spoofed caller ID calls may be used to trick you into giving up personal information, such as your Social Security number or credit card information. Display differs from stored contact: Another warning sign of a spoofed phone number is if the display name differs from your stored contact information. For example, if you have your friend listed as “Dave Smith” on your phone but receive a call from “David Smith,” it may be a spoofed call. If you notice one or more of these warning signs when dealing with an incoming call, it's best to treat it as a spoofed phone call and ignore it. How to avoid caller ID spoofing: 8 protection tips Now that you know what to look out for, here are some protection tips you can utilize to avoid caller ID spoofing and the scams that may be associated with it. Avoid answering unknown numbers: Even if the caller ID display name seems familiar, avoid answering calls from unknown numbers, as they could be a scammer in disguise. Don’t hit any buttons: If you happen to answer a spoofed call, avoid pressing buttons or following any of their instructions. Instead, hang up immediately. Stay silent: If you end up answering a call you’re unsure about, it’s best to stay silent and hang up to avoid accidentally giving up any personal information. Keep your information private: Whenever you’re talking to someone you don’t know, be sure to avoid sharing any personal information, as a scammer could use it for malicious purposes such as identity theft. Enable spam-blocking features: To help minimize spam texts and calls from unknown phone numbers, be sure to enable your device’s spam-blocking features. This can help prevent a spoofed call from reaching your phone, even if the display name is familiar. Secure your voicemail inbox: Some scammers may even attempt to spoof your phone number to call others and access your voicemail inbox. To help stop them, be sure to secure your voicemail box with a password. Redial the number yourself: If you’re ever suspicious that you’re receiving a spoofed call, hang up and dial the number back yourself to ensure you are actually speaking to a legitimate caller. Block suspicious callers: By blocking any suspicious or unknown callers, you can reduce the number of unwanted calls your phone receives. To block caller ID spoofed calls on an iPhone, follow these steps: Open the Phone app. Tap “Recents.” Select the info button () next to the phone number you’d like to block. Scroll down and select “Block this Caller.” Tap “Block Contact.” To block spoofed calls on an Android, follow these steps: Open the Phone app. Select “Recents.” Long press the phone number you’d like to block. Tap “Block/report spam.” Check the “Report call as spam” box. Select “Block.” Even after prioritizing all these detection and prevention tips, it’s still possible that a spoofed phone call can slip through the cracks. What to do if your number is spoofed While receiving spoofed calls can be annoying, having your own name or number spoofed can be even worse. If you start to hear that your identity is being used for spoof calls that you aren’t making yourself, follow these steps: Set a new voicemail message: To help clear up any confusion, be sure to record a new voicemail message explaining the situation. That way, anybody who calls you will know that your number has been spoofed, and it isn’t you who has been contacting them. Block or silence all unknown callers: Using either a call-blocking service or your phone’s settings, block or silence all unknown callers. This can help minimize the annoyance of random people calling you thinking that they are going to reach someone else. Report the situation to the FCC and your local authorities: To help stop telephone spoofing, be sure to file a complaint with the FCC and inform your local authorities. Now that you’ve learned how to detect and avoid caller ID spoofing and what you can do if your number is spoofed, you can help minimize the risk of engaging with a spoofed phone call. To better increase your Cyber Safety, educate yourself on the other mobile scams that can make their way to your device. FAQs about caller ID spoofing Still curious about caller ID spoofing? Read along to learn the answers to some of the most frequently asked questions about caller ID spoofing. Is caller ID spoofing illegal? It depends. As a result of the Truth in Caller ID Act of 2009, it is illegal for any person in the United States to use caller ID spoofing with the intent to defraud, steal, or cause harm. Because of this, caller ID spoofing is legal as long as there is no ill intent. For example, businesses may legally alter their caller ID to list a toll-free callback number, even if it’s not the number they are calling from. Why is caller ID spoofing dangerous? While caller ID spoofing may seem like a harmless prank, scammers can use this technique for malicious purposes, such as different types of phishing attacks. For example, a scammer may pose as a trusted entity to get you to give up sensitive information that can be used to steal your identity, money, or login information. What is neighbor spoofing? Neighbor spoofing is a type of caller ID spoofing in which the scammer impersonates a phone number like your own in hopes you’ll be more likely to answer. For example, if your phone number is (555) 555-0101, you may receive a call from (555) 555-0102. What is blocking or labeling on your caller ID? Blocking or labeling on your caller ID is when an incoming call is automatically blocked or labeled as “potential spam,” “spam,” or another similar description, depending on your device. This is because the FCC allows telephone providers to automatically block phone numbers proven to be used for spam purposes. Do telemarketers have caller ID rules? Yes. All telemarketers must provide the appropriate number from which the phone call is coming. In addition, the phone number must be reachable during regular business hours in case you’d like to call and request that they no longer contact you. Can you find out who spoofed your number? Unfortunately, it is very difficult to find out who exactly has been spoofing your number. Depending on the specific method the scammer used, tracking down who has been spoofing your number may only be possible by contacting law enforcement or your telephone company. What are the legitimate reasons for caller ID spoofing? Are you afraid of losing your personal information or all the precious things on your computer? Get comprehensive protection with Norton Security Deluxe across all your devices – up to 5 PCs, Macs, smartphones or tablets. Create an account today and try it free for 30 days on up to 5 of your devices. While caller ID spoofing is commonly used by scammers, there are instances in which it is used legitimately. For example, those involved in journalism or law enforcement may decide to use caller ID spoofing to privately place calls without disclosing their identity, phone number, or location. Editorial note: Our articles provide educational information for you. Our offerings may not cover or protect against every type of crime, fraud, or threat we write about. Our goal is to increase awareness about Cyber Safety. Please review complete Terms during enrollment or setup. Remember that no one can prevent all identity theft or cybercrime, and that LifeLock does not monitor all transactions at all businesses. The Norton and LifeLock brands are part of Gen Digital Inc.