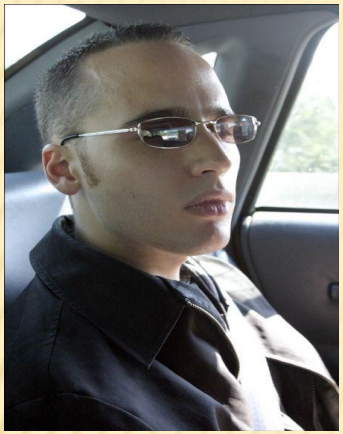
ХАКЕРЫ

Адриан Ламо, Кевин Митник и Кевин Поулсен



Адриан Ламо (род. 20 февраля 1981)

Ламо использовал соединения с интернетом повсеместно: в кафе и библиотеках, для улучшения своих навыков. Благодаря этому он заработал себе прозвище «Бездомный Хакер».

Список побед Ламо включает такие компании, как **Microsoft, New York Times, AOL, Sun Microsystems, Yahoo!, MacDonald's, Cingular, Citigroup, Bank of America.**

Ламо действовал, нарушая законы. По мнению коллег-хакеров, атаки Ламо на известные корпорации мотивируются прежде всего жаждой всеобщего внимания и славы.

Вторжение Ламо в сеть **NY Times** в **2002** году привлекло к нему внимание противников киберпреступности. Суд назначил ему выплатить **$65 000** в качестве компенсации. В дополнение, он был приговорён к **6** месяцам домашнего ареста и **2** годам испытательного срока.

В настоящий момент Ламо является известным лектором и журналистом, независимым консультантом по безопасности

В конце мая **2010** года Ламо донёс властям США про то, как военнослужащий Брэдли Мэннинг вместе с другими документами передал **WikiLeaks** запись расстрела американским военным вертолётом группы гражданских в Ираке (Мэннинг рассказал об этом Ламо в доверительной беседе). После этого Мэннинг был арестован.

Кевин Поулсен (род. 1965), более известный как **Dark Dante.**

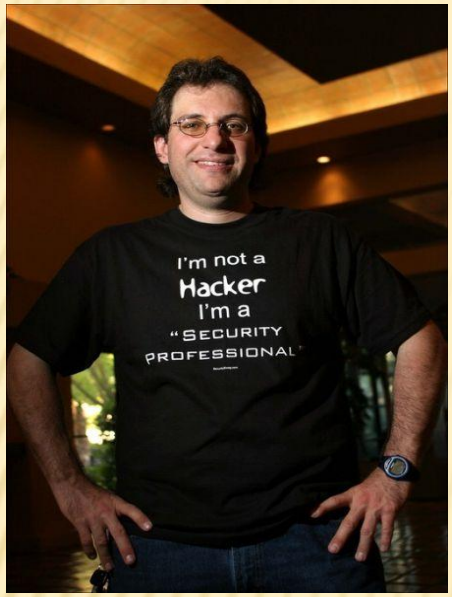
В **1983** году, когда ему было всего **17** лет, он начал заниматься взломом различных сетей, что привело к нескольким стычкам с правовой системой США.

Впервые его арестовали в **1989** году, когда ему было **24** года. Тогда его обвинили в нескольких взломах телефонных сетей и компьютерных серверов, против него были собраны разные уличающие доказательства. Но когда пришло время предстать перед судом, Поулсен решил скрыться, агенты ФБР **17** месяцев выслеживали его, пока в апреле **1991** года его не арестовали.

В **1994** году Кевин Поулсен был приговорён к четырём годам тюремного заключения.

С момента выхода из тюрьмы Поулсен работал в качестве журналиста и был повышен до поста главного редактора **Wired News.**

Кевин Дэвид Митник (род.6 августа 1963)



Он создал себе имя в **1981** году, будучи ещё семнадцатилетним подростком, и прославился тем, что взламывал телефонные сети, перенаправляя вызовы абонентов по собственному желанию.

Самый большой успех пришёл к Кевину Митнику в **1983** году, когда он совершил поистине впечатляющее деяние. В то время он был студентом южнокалифорнийского университета. Используя один из университетских компьютеров, Митник проник в глобальную сеть **ARPANet**, являющуюся предшественницей **Internet**, которая в то время была предназначена для военных целей и объединяла крупные корпорации и университеты.

Проникнув в эту сеть, Митник добрался до самых защищённых компьютеров того времени, до компьютеров Пентагона. Он получил доступ ко всем файлам Министерства обороны США.

В то время не было никаких следов кражи информации или порчи: Митник действовал просто из любопытства и проверял свои способности.

Но один из системных администраторов обнаружил акт вторжения и поднял тревогу. Расследование выявило автора атаки, и Кевина Митника арестовали прямо на территории университета.

Он был осуждён и отбыл своё первое настоящее наказание за незаконное вторжение в компьютерную систему, проведя полгода в исправительном центре для молодёжи.

В **1987** году Кевин Митник вместе со своим другом Ленни ДиСикко вторгся во внутреннюю сеть исследовательской лаборатории американской компьютерной компании **Digital Equipment Corporation (DEC).**

Для Митника сделать это было несложно**,** так как ДиСикко являлся сотрудником данной лаборатории и одновременно был соучастником взлома**. EasyNet -** внутренняя сеть **DEC -** не выдержала хакерской атаки**,** и вскоре сообщники получили доступ ко всей системе**.**

На этот раз Митник взломал систему не из простого любопытства или для проверки своих способностей**:** у него было другая цель**.** Хакер хотел завладеть исходным кодом операционной системы **VMS,** разработанной компанией **DEC** для компьютеров **VAX.**

Судебное дело длилось недолго**:** компания **DEC** обвинила хакера в краже информации и запросила за нанесённый ущерб более **$200 000.**

Митника приговорили к одному году тюремного заключения**,** кроме того**,** он должен был посещать шестимесячные курсы для излечения от компьютерной зависимости**.**

В **1994** году Кевин Митник вернулся к своей незаконной деятельности.

Неоднократно совершённые преступления вынудили ФБР начать на него **"охоту".**

На Кевина Митника была объявлена облава, самая впечатляющая за всю историю поимки хакеров.

Федералы разослали повсюду его фотографии, чтобы узнавшие его люди могли позвонить властям.

U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).
United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: .....MITNICK, KEVIN DAVID
AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:
Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: ...DOPM2OPM13DIPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS

VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-2485).
If no answer, call United States Marshals Service Communications Center in McLean Virginia, Telephone (800)336-0102; (24 hour telephone contact) NLETS access code is VAUSMOOOO.

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED

Form USM-132 (Rev. 3/85)

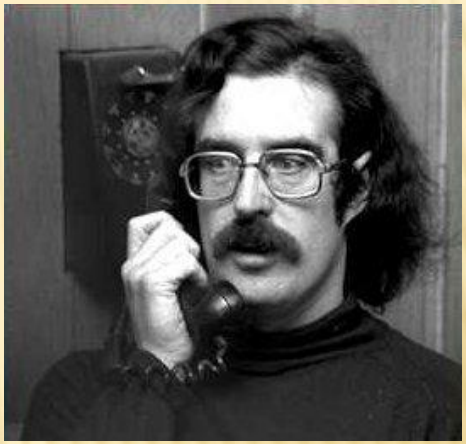
November 1992

В **90-**е гг. Кевин Митник был приговорён к пяти годам тюремного заключения.

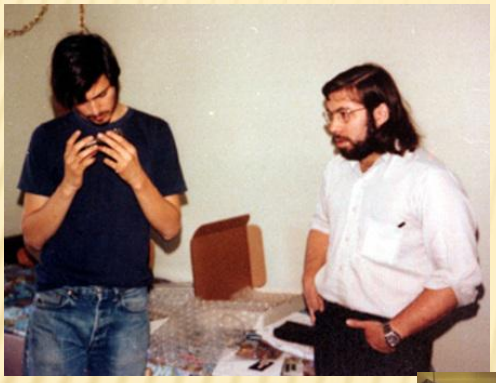
Кевин Митник арестован

На сегодняшний день Митник является специалистом по безопасности и владельцем собственной компании **Mitnick Security Consulting.**

Джон Дрейпер (родился в 1944 году)

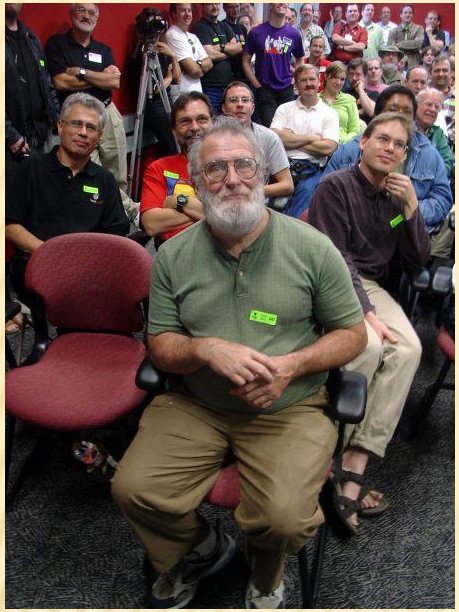


Более известный как **Cap'n Crunch,** начал свою хакерскую деятельность в конце **60-**х гг**.** и был одним из первых хакеров**.**



Джон вместе со своими друзьями Стивом Возняком и Стивом Джобсом создали устройство**,** названное **"Blue Box",** позволяющее имитировать звуки телефонной сети и осуществлять бесплатные звонки**.**

В **1972** году Джона Дрейпера арестовали**.** Судебное преследование длилось долго**,** потому что это был первый случай в истории**,** когда правовая система имела дело с таким типом мошенничества**.** Спустя четыре года Дрейпера приговорили к двум месяцам тюремного заключения**.**



Деятельность Джона Дрейпера породила целое движение, связанное с фрикингом - уклонением от платы за телефонные переговоры.

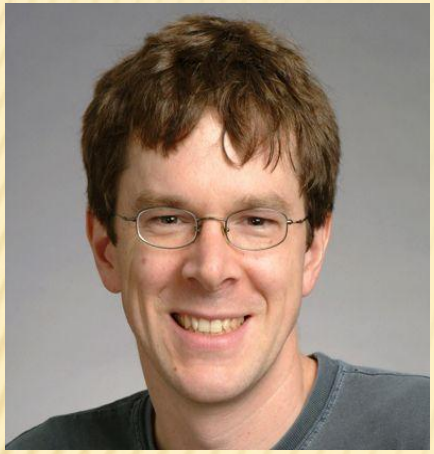
Появилась группа хакеров и фрикеров, давшая себе название **«2600».**

Джон Дрейпер известен как автор программы, которая была первым в мире текстовым редактором для **IBM PC.**

В настоящее время он возглавляет собственную компанию, специализирующуюся на разработке систем защиты от спама, отражения хакерских атак и обеспечении безопасности персональных компьютеров.

Дрейпер входит в группу ведущих исследователей в области информационной безопасности. Он является разработчиком программного комплекса **Crunchbox,** обеспечивающего комплексную защиту от сетевых атак.

Роберт Таппан Моррис (род. 8 ноября 1965 г.)



2 ноября **1988** г. зафиксирован первый случай появления и «победоносного» шествия сетевого червя, парализовавшего работу шести тысяч интернет-узлов в США.

Позднее в СМИ этот червь был наречён червём Морриса по имени его автора (аспиранта факультета Вычислительной техники Корнелльского университета – Роберта Т. Морриса) Хакеры прозвали его «великим червём».

Концепция "червя" несколько отличается от классического хакерства, однако "черви" действуют по тому же принципу, но вместо того чтобы влезать в сеть самому, хакер отправляет маленькую программу, запрограммированную на выполнение определённых задач.

По словам Морриса, основной целью его программы было оценить истинные размеры сети Интернет, т.е. определить количество подключённых к ней компьютеров. В то время к Интернету было подключено не так много машин, но вопреки расчётам Морриса, его "червь" причинил гораздо больше вреда, чем ожидалось.

"Червь" Морриса был запрограммирован на то, чтобы проверить компьютер и скопировать себя в систему, если машина ещё не была инфицирована. Но, позднее он модифицировал код программы, чтобы "червь" оставлял свои копии каждый раз, независимо от того, инфицирован компьютер или нет.

"Червь" Морриса распространился, как пожар, заразив несколько тысяч компьютеров всего за несколько часов.

Приблизительно подсчитали, что восстановление каждой инфицированной системы будет стоить от **$200** до **$53 000**, в зависимости от компьютера.

Чтобы остановить "червя", были мобилизованы различные команды программистов, для нейтрализации атаки понадобилось несколько дней.

Роберт Таппан Моррис был признан виновным в компьютерном мошенничестве и был приговорён к трём годам условно, **400** часам общественных работ и **$10 050** штрафа.

Сейчас Роберт Моррис является штатным профессором Массачусетского технологического института (МТИ) в лаборатории компьютерных наук и искусственного интеллекта.

Джонатан Джозеф Джеймс

(12 декабря 1983 — 18 мая 2008) — американский хакер.

Джонатан стал широко известен благодаря тому, что стал первым несовершеннолетним, отправленным в тюрьму за «хакерство» в США. Ему было **15** лет во время первого нарушения и **16** лет в день оглашения приговора.

29 и **30** июня **1999** года этот несовершеннолетний хакер навёл страх на НАСА с помощью простого компьютера **Pentium.**

Взломав пароль сервера, принадлежащего Агентству по сокращению военной угрозы, которое является частью Министерства Обороны США, Джеймс смог свободно бродить по сети и украсть несколько файлов, включая исходный код международной орбитальной станции.

После обнаружения взлома НАСА пришлось отключить систему для проверки и приведения её в рабочее состояние, что обошлось в **$41000.**

Поймали Джеймса быстро, так как НАСА сделало всё, чтобы его остановить.

По заявлению НАСА, стоимость украденного Джеймсом программного обеспечения оценивается в **1,7** млн долларов.

Однако молодой возраст Джеймса помог ему избежать тюрьмы. По оценкам адвокатов, будь преступник совершеннолетним, за кражу суперсекретных документов ему грозило бы, как минимум, десять лет тюремного заключения.

18 мая **2008** года Джеймс умер. По некоторым данным - убран государственными структурами.

Гэри Мак Киннон

(родился **10** февраля **1966** года)
— шотландский хакер (британский подданный).

В **2001-2002** годах взломал компьютеры, принадлежащие армии, ВМС, Министерству обороны, ВВС и Пентагону.

В общей сложности Мак Киннон получил несанкционированный доступ к **97** компьютерам, и каждый раз он искал в них информацию о летающих тарелках.

Его атаки были самыми крупными из когда-либо зафиксированных военными США.

Мак Киннон уничтожил секретную информацию и сорвал множество военных операций, суммарный ущерб нанесенный им США оценивается в **$900** тысяч.

Правительству США не понадобилось много времени, чтобы выйти на Мак Киннона и начать преследование. Мак Киннон был пойман в **2002** году, после того как одна из использованных им программ вывела следователей на адрес электронной почты его девушки.

США потребовали экстрадиции Мак Киннона.

Адвокаты Мак Киннона надеялись, что он будет отбывать наказание в Британии, но суд все-таки вынес решение об его экстрадиции.

Владимир Леонидович Левин

(родился в 1967 году)

- первый известный во всем мире российский хакер

В **1994** году он проник во внутреннюю сеть американского банка **Citibank,** взломав аналоговое модемное подключение банка и получив доступ к нескольким счетам**.**

Он сумел перевести **10,7** миллиона долларов на счета в США**,** Финляндию**,** Германию**,** Израиль и Нидерланды**.**

Левину помогали трое сообщников**,** которых арестовали**,** когда они пытались стащить украденные деньги**.** Их допрос вывел на след Левина**,** который работал программистом в Санкт-Петербурге**.**

Российского хакера арестовал в марте **1995** года в лондонском аэропорту Хитроу Интерпол**.**

Судебное разбирательство против него началось только в сентябре **1997** года**.**

Левина приговорили к трём годам лишения свободы**,** которые он отсидел в американской тюрьме**.**

Мурат Уртембаев - первый хакер в истории СССР

В **1983** году в СССР было совершенно первое в истории преступление в сфере высоких технологий – хакнул ПО на АвтоВАЗе, в результате чего конвейер встал на три дня.

Бороться с ЧП были брошены лучшие специалисты. Конвейер удалось запустить лишь через три смены.

Мурат Уртембаев сам пришел на явку с повинной. Если бы первый хакер СССР не признался, то его имя осталось бы загадкой для истории АвтоВАЗа.

Возник прецедент: совершено преступление, за которое не предусмотрено наказание.

Статьи, которая в нынешнем УК квалифицируется деяние Уртембаева, как «создание, использование и распространение вредоносных программ для ЭВМ» и предусматривает лишение свободы на срок от трех до семи лет, тогда еще не было.

Первого хакера в нашей истории осудили за умышленные хулиганские действия и дали полтора года условно с возмещением ущерба, который был оценен в стоимость двух «Жигулей».

Дело получило широкую огласку в СССР. Правоведы, партийные руководители, специалисты – все спорили друг с другом, пытаясь доказать считать или не считать действия Уртембаева преступлением.

* * *

В **1998** году российский хакер Илья Гофман взломал сайт канадского интернет-магазина.

Деньги клиентов он переводил на собственные пластиковые карты, после чего при помощи друзей обналичивал.

Более года просидел в следственном изоляторе «Матросская тишина» и получил условный срок - **5** лет.

* * *

В **1996** году группа программистов-взломщиков «вскрыла» шесть банков в США на **2** миллиона долларов. А в ноябре **99**-го дерзкая атака на расчетную систему **Bank of America** нанесла ущерб в **$30** миллионов.

В обоих случаях виновников так и не нашли. ФБР только и сумело выяснить, что след ведет в Россию.

* * *

В январе **2007**-го российские хакеры на целый день «заморозили» работу одного из самых защищенных американских сайтов - страницу ФБР.

* * *

В начале **2007**-го группа хакеров-антифашистов из разных городов России провела атаку на наиболее известные интернет-форумы, где общаются скинхеды. Кодовые имена, пароли и явки были переданы спецслужбам.

* * *

1 мая **2007** года были взломаны сайты министерства обороны и МВД Эстонии, а также официальный сайт президента этой страны. Сайты «лежали» двое суток.

Эту акцию наши хакеры провели в знак протеста против переноса Бронзового Солдата с площади.

12 февраля **2004** года был самый обычный день**,** но в компании **Microsoft** было объявлено чрезвычайное положение**.** Кто**-**то украл исходный код операционной системы **Windows 2000,** которой до сих пор пользуется большое количество пользователей**.** И что ещё хуже**,** неизвестный хакер выложил этот код в **Wild.**

Кража была масштабна**: 600** миллионов байт данных**, 30 195** файлов и **13,5** миллиона строк кода**.** Утечка информации коснулась операционной системы **Windows 2000** и её **"**старшей сестры**" Windows NT4.** Все сотрудники **"**софтового**"** гиганта пытались выяснить**,** что произошло**,** но никто не мог дать ответ**.**

Данные были украдены прямо из сети **Microsoft.** Неизвестный хакер вошёл во внутреннюю сеть компании**,** взломав пароль одного из компьютеров**.** Исходный код быстро распространился по Интернету**,** особенно по **P2P-**сетям**.** К счастью**,** несмотря на то**,** что все опасались худшего**,** последствия этой грандиозной кражи оказались довольно мягкими**.**

Хакерские атаки происходят регулярно и узнать о последних можно на сайте

hacker.report.ru

Эмблема хакеров — предложена в октябре **2003** года Эриком Рэймондом, как символ отношения к хакерской культуре.

На эмблеме изображён **«**планер**»** (англ. ***glider***) — одна из фигур игры **«**Жизнь**»**.

Эрик Рэймонд подчёркивает, что демонстрация данной эмблемы не означает, что носитель объявляет себя хакером, поскольку хакером нельзя объявить самого себя: это титул, который присваивается сообществом. Использование эмблемы, однако, означает, что носитель разделяет цели и ценности хакерского сообщества.

Данная эмблема не является изображением, защищённым авторским правом, или товарным знаком, и её использование в коммерческих целях хоть и не поощряется, но и не запрещается.

Идея использования моделей из **«**Жизни**»** в качестве символов высказывалась до предложения Эрика аргентинским хакером Себастьяном Вэйном в марте **2003.**

Глайдер удовлетворяет критериям хорошего логотипа. Он прост, смел, его трудно перепутать с чем бы то ни было и легко нанести на кружку или футболку. Его можно варьировать, комбинировать с другими эмблемами, его можно превратить в повторяющийся фоновый рисунок.