Некоторые опасности постоянно включённого NFC (Near Field Communication - связь в ближнем поле) в телефоне:

- **Отсутствие двухфакторной проверки.** Если телефон украдут, то злоумышленник может спокойно оплачивать покупки без подтверждения.
- **Случайная покупка.** Модуль NFC может отреагировать на терминал рядом и оплатить покупку, которая не планировалась.
- **Кража денег.** В толпе неизвестные могут приблизиться настолько, чтобы украсть данные и деньги со смартфона, на котором активирован NFC. Расстояние 10-45 см.
- **Передача вредоносного ПО.** Через NFC-модуль может быть передано вредоносное программное обеспечение, которое будет считывать данные с карты и передавать их мошеннику.

Троян NGate на платформе Android распространяется он через фишинговые сообщения или замаскированные утилиты. Он клонирует данные карт жертв, после чего позволяет мошенникам производить несанкционированные платежи и даже снятие наличных средств в банкоматах.

При этом злоумышленнику не обязательно находиться рядом — данные передаются через серверы.

Зачем отключать Bluetooth

Атаки на Bluetooth — обычное явление. Злоумышленники активно пользуются этим, поэтому взломы можно разделить на три вида.

Bluejacking — атака, во время которой мошенник использует соединение для проникновения в телефон и отправки анонимных сообщений на другие устройства, находящиеся по близости. Такие атаки могут использовать для дорогостоящих звонков в другие страны.

Bluesnarfing — взлом, сопровождающийся кражей конфиденциальной информации, например, интернет-аккаунтов, фотографий, видео. Делается это все очень быстро, пока есть возможность «сработать» в пределах досягаемости.

Bluebugging — самый худший вариант, при котором взломщик имеет возможность контролировать ваше устройство, прослушивать смартфон и получать доступ ко всем данным, которые есть в памяти.

Чем могут быть опасны Wi-Fi-сети?

Ответ прост: кражей данных. Пользуясь Интернетом, вы передаете много ценной информации — платежные данные, логины и пароли от всевозможных сервисов, документы и переписку. Если она попадет в руки преступника, он сможет перевести все ваши банковские накопления на свой счет, украсть ваши аккаунты и распространять через них спам или выпрашивать у ваших знакомых деньги. Добравшись до личной переписки, он способен вас шантажировать.

Не доверяйте общественным Wi-Fi-сетям, помните, что не требующие пароля Wi-Fi-сети подходят лишь для вылазок в Интернет, не связанных с важной информацией: данные, которые вы передаете и получаете через них, может подсмотреть любой, кто получит доступ к той же сети.

Что делать, чтобы избежать потери важных данных:

- отключайте Wi-Fi, когда им не пользуетесь.
- запретите автоматическое подключение к сетям (обычно это можно сделать в настройках Wi-Fi).
- удаляйте («забывайте») общественные сети Wi-Fi из списка подключений сразу, как закончите ими пользоваться.
- не используйте недоверенный Wi-Fi для работы с сервисами, требующими аутентификации.

В идеале заходить в любые аккаунты, где хранятся важные данные (особенно касающиеся финансов), следует исключительно в защищенной среде домашнего или корпоративного Интернета. Но если обстоятельства вынуждают срочно проверить баланс карты или залогиниться на госуслугах, то делайте это через мобильную связь. Даже если дорого и в роуминге — утечка конфиденциальной информации через сомнительную Wi-Fi-точку обойдется вам гораздо дороже.

Чаще всего хакеры устанавливают снифферы в местах распространения незащищенного подключения Wi-Fi, например, в кафе, отелях и аэропортах. Снифферы могут маскироваться под подключенное к Сети устройство.

Перехватить трафик через сниффер можно следующими способами:

- путем прослушивания в обычном режиме сетевого интерфейса.
- подключением в разрыв канала и перенаправлением трафика.
- с помощью анализа побочных электромагнитных излучений.
- при помощи атаки на уровень канала и сети, приводящей к изменению сетевых маршрутов.

Сниффер (от англ. to sniff — «нюхать») — это устройство или программное обеспечение, позволяющее считывать, анализировать, а в случае злонамеренности и искажать, сетевой трафик в месте собственного подключения к сети.

Как обычно взламывают пароли.

Начнем с важной ремарки: под фразой «взломать пароль» мы подразумеваем взлом его хеша — уникальной последовательности символов. Дело в том, что почти всегда пользовательские пароли хранятся на серверах компаний одним из трех способов.

- **В открытом виде.** Это самый простой и понятный способ: если у пользователя пароль, например, qwerty12345, то на сервере компании он так и хранится: qwerty12345. В случае утечки данных злоумышленнику для авторизации не потребуется сделать ничего сложнее, чем просто ввести логин и пароль. Это, конечно, если нет двухфакторной аутентификации, хотя и при ее наличии мошенники иногда могут перехватывать одноразовые пароли.
- **В закрытом виде.** В этом способе используются алгоритмы хеширования: MD5, SHA-1 и другие. Эти алгоритмы генерируют для каждой парольной фразы уникальное хеш-значение — строку символов фиксированной длины, которая и хранится на сервере. Каждый раз, когда пользователь вводит пароль, введенная последовательность символов преобразуется в хеш, который сравнивается с хранящимся на сервере: если они совпали, значит, пароль введен верно. Приведем пример: если в реальности ваш пароль qwerty12345, то «на языке SHA-1» он будет записываться вот так —

4e17a448e043206801b95de317e07c839770c8b8. Когда злоумышленник получит этот хеш, ему потребуется его дешифровать (это и есть «взлом пароля»), например, с помощью радужных таблиц, и превратить обратно в qwerty12345. Узнав пароль, хакер сможет использовать его для авторизации не только в сервисе, с которого утек хеш, но и в любом другом, где используется этот же пароль.

- **В закрытом виде с солью.** В этом способе к каждому паролю перед хешированием добавляется соль — случайная последовательность данных, статическая или формирующаяся динамически. Хешируется уже последовательность *«пароль+соль»*, что меняет результирующий хеш, а значит, существующие радужные таблицы уже не помогут хакерам. Такой способ хранения паролей значительно усложняет взлом.

Для нашего исследования мы собрали базу из 193 млн слитых паролей в открытом виде. Откуда мы ее взяли? ~~Места надо знать.~~ Нашли в сети даркнет — там они зачастую находятся в свободном доступе. Мы используем такие базы, чтобы проверять пользовательские пароли на предмет возможной утечки, при этом ваши пароли мы не знаем и не храним: вы можете подробнее узнать, как устроено изнутри хранилище паролей в Password Manager и как, не зная ваших паролей, мы сравниваем их с утекшими.

Сколько стоит взломать пароль

Лучше всего с анализом стойкости паролей справляются современные графические процессоры. Например, для видеокарты RTX 4090 скорость подбора с помощью инструмента восстановления пароля hashcat составляет 164 гигахеша в секунду при взломе «соленых хешей», созданных с использованием алгоритма MD5.

Предположим, что взламываемый пароль состоит из 8 знаков, для каждого из которых может быть использован один из 36 различных символов (латинские буквы одного регистра и цифры). Количество возможных уникальных комбинаций при этом — 2,8 трлн (посчитать это можно, возведя 36 в восьмую степень). Методом полного перебора (**брутфорсом**) современный процессор с вычислительной мощностью 6,7 млрд хешей в секунду взломает такой пароль за **7 минут**. А вот упомянутая выше RTX 4090 справится с задачей всего за **17 секунд**.

Стоит такая видеокарта чуть меньше 2000 долларов, но, даже если у злоумышленника нет возможности ее купить, он может практически без проблем арендовать вычислительную мощность всего за несколько долларов в час. А что, если ему придет в голову арендовать сразу десяток RTX 4090? Мощности хватит, чтобы без проблем обрабатывать гигантские утечки баз.

59% паролей могут быть взломаны менее чем за час

В исследовании мы проверяли стойкость паролей, используя как **брутфорс**, так и алгоритмы умного взлома. И если **брутфорс** перебирает все возможные комбинации символов по порядку, пока не найдет совпадение, то умные алгоритмы обучаются на базе данных паролей и умеют рассчитывать частотность различных комбинаций символов, начиная перебор с наиболее популярных вариантов и заканчивая редко встречающимися. Подробнее об использованных алгоритмах можно прочитать в полной версии нашего исследования на Securelist.

Результаты неутешительны: 45% из 193 млн изученных реальных паролей (то есть 87 млн!) могут быть взломаны умными алгоритмами менее чем за одну минуту, 59% — за один

час, а 67% — менее чем за месяц, и всего 23% паролей можно считать стойкими — их взлом займет более одного года.

Время взлома	Процент паролей, которые возможно взломать указанным методом	
	Брутфорс	**Умный взлом**
До минуты	10%	45%
От минуты до часа	+10% (20%)	+14% (59%)
От часа до дня	+6% (26%)	+8% (67%)
От дня до месяца	+9% (35%)	+6% (73%)
От месяца до года	+10% (45%)	+4% (77%)
Более года	+55% (100%)	+23% (100%)

Важно отметить, что подбор *всех* паролей из базы данных занимает ненамного больше времени, нежели подбор *одного* пароля. Ведь на каждой итерации, рассчитав хеш для очередной комбинации символов, злоумышленник проверяет, есть ли такой же в базе данных. Если да, то соответствующий ему пароль помечается как «взломанный», после чего алгоритм продолжает подбирать другие пароли.

Почему алгоритмы умного взлома так эффективны

Люди редко используют случайные пароли и генерируют их в своей голове гораздо хуже машин: мы используем реальные фразы, личные имена и последовательности, для разгадывания которых как раз и существуют алгоритмы умного взлома.

Более того, даже если попросить нескольких человек выбрать любое число от 1 до 100, то большинство людей назовут… одни и те же числа! Исследователи с YouTube-канала Veritasium опросили более 200 тысяч человек и выяснили, что 7, 37, 42, 69, 73 и 77 — в топе популярности.

И даже если вы попытаетесь придумать пароль из случайных символов, то неосознанно будете чаще всего выбирать буквы в середине клавиатуры. Большинство исследованных нами паролей (57%) содержат слово из словаря, что существенно снижает их стойкость. На взлом половины (51%) таких паролей потребуется меньше минуты, 67% — можно будет подобрать менее чем за час, и лишь 12% из них являются стойкими — на их подбор уйдет более года. Также, к счастью, всего несколько паролей состояли исключительно из словарного слова — практически все из них могут быть взломаны за минуту. Больше о том, какие схемы паролей нам попадались, — в публикации Securelist.

Умные алгоритмы без труда разбираются с большинством паролей, содержащих словарные последовательности. Более того, они учитывают даже замены символов, поэтому написание «pa$$word» вместо «password» или «@dmin» вместо «admin» не сделает пароль более стойким. Использовать популярные слова и последовательности цифр — тоже плохая идея. В 4% обработанных нами паролей в разном виде встречались:

- 12345
- 123456
- love
- 12345678

- 123456789
- admin
- team
- qwer
- 54321
- password

Рекомендации

Это практическое исследование позволяет сделать много выводов о стойкости паролей:

- Пароли многих пользователей недостаточно сильные, 59% из исследованных паролей могут быть взломаны за один час.
- Использование слов, имен и стандартных последовательностей в пароле уменьшает время его подбора.
- Самые небезопасные пароли полностью состоят либо из цифр, либо из словарных слов.

Также мы подготовили простые рекомендации, которые помогут сделать ваши аккаунты защищеннее:

- Генерируйте надежные пароли с помощью Password Manager.
- Если решили создавать пароль самостоятельно, то используйте мнемонические фразы, а не осмысленные словосочетания, имена и словарные последовательности.
- Не используйте один и тот же пароль на разных сайтах, потому что далеко не все компании хранят пользовательские данные безопасно.
- Никогда не сохраняйте пароли в браузерах.
- Храните все свои пароли в менеджере паролей и не забудьте придумать для него взломостойкий мастер-пароль.
- Проверьте устойчивость своего пароля к взломам с помощью Password Checker или же прямо в менеджере паролей, который найдет все слабые и дублирующиеся пароли, проверит все ваши пароли по базам скомпрометированных и уведомит при нахождении совпадений.
- Включайте двухфакторную аутентификацию (2FA) везде, где это возможно.