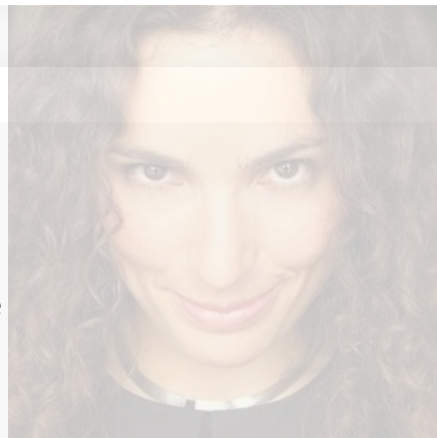


Пароль лесенкой или Показательная история про «взломанный ящик»

Вице-президент Mail.Ru Group Анна Артамонова рассказала в фейсбуке о вреде использования одинаковых паролей для разных сервисов и о пользе двухфакторной аутентификации.

Анна Артамонова
Вице-президент Mail.Ru Group



Буду тут рассказывать без имен все показательные истории про «взломанные ящики», с которыми ко мне обращаются многочисленные знакомые и знакомые знакомых.

Что характерно, чаще всего, это не новички интернета (я вообще не знаю, остались ли еще такие), не жители сел и деревень. Это люди нашего с вами круга (IT, медиа и вот это вот все), в интернете 5+ лет, уверенные, как говорится, пользователи, иногда даже профессионалы.

Кстати, знаете в чем характерное отличие таких пользователей от вашей мамы или бабушки? :) Нет, не не угадали! Не в том, что они себя ведут более осмотрительно, а в том, что мама, словив вирус, считает, что «я, балда, не доглядела», а «опытный пользователь», профукав пароль, чаще всего кричит «криворукие программисты сервиса X виноваты!».

«Злоумышленник просто знал пароль»

Вот, собственно, последний случай: обращается продюсер известных звезд, говорит «у меня сменили пароль! мне пришла об этом смс-ка (то есть телефон подключен, что уже хорошо), я никому не сообщал этот пароль и он у меня очень хитрый, слава богу, я успел его оперативно восстановить через привязанный телефон».

Смотрим, что происходило вчера с его ящиком: в ящик был вход по паролю «XXXX» и смена пароля (как мы теперь понимаем, злоумышленником). После чего восстановление пароля через телефон (видимо хозяин) и смена пароля (хозяин).

То есть никаких попыток взлома или брутфорса, злоумышленник просто знал пароль и вошел с первой попытки (собственно, для системы он в таком случае выглядит как сам пользователь).

Спрашиваем продюсера «использовал ли ты, дорогой, этот пароль еще где-то»? «Нет, — говорит, продюсер, » вы что! Я очень ответственный...ну хотя, только на фейсбук такой же пароль, но не могли же у фейсбука украсть!».

Поскольку у нас пароли хранятся в виде соленых хешей, то посмотреть их не может никто, даже сотрудник нашей службы безопасности. Зато он может поискать емейл-жертву в различных базах аккаунтов, от взломов различных сервисов, которые во множестве доступны в даркнете (и мы их внимательно мониторим). И что же! «Хитрый пароль, который никому не сообщался», подходивший к аккаунту, обнаруживается сразу в нескольких базах — это и дампы социальных проектов и интернет-магазинов. Где его только нет. То есть реально, любой юный хакер, скачав базу за 10 долларов, мог войти в этот ящик по валидному паролю.

«Лучше уж на бумажке записывать!»

А как же мониторинг баз, вы же ищите и блокируете все совпадения? – спросите вы. Хороший вопрос! Это действительно так, как только мы находим свежую базу чужих взломанных аккаунтов с емейлами, мы проверяем ее содержимое на валидность у нас, и, в случае совпадения, ставим ящику статус «заблокирован», чтобы злоумышленники не могли в него войти, а восстановить мог только хозяин.

Так вот, когда все эти базы проверялись, у ящика был другой пароль! Который тоже был скомпрометирован таким же образом (то есть тоже встречался в таких базах). Мы ящик заблокировали около месяца назад, после чего человек разблокировал ящик и поставил «новый» пароль, который на деле оказался не таким уж новым и тоже был прилично засвечен в сети. Короче поменял шило на мыло.

Человеку повезло, что он в какой-то момент все-таки догадался привязать к ящику мобильный телефон, благодаря чему, восстановление доступа прошло для него практически безболезненно.

А теперь подумайте, кто из вас узнал в этом человеке себя. Небось тоже имеете три пароля «старый», «новый» и «еще новее» и используете без разбору во всех сервисах? Вам тоже кажется, что самый старый пароль уже «давно нигде не использовался, поэтому можно снова начать»? Нет ребята, так не работает. Интернет, он все помнит. Скорее всего, ВСЕ ваши старые пароли утекли когда-нибудь из старых говносайтов и форумов и болтаются где-то в базах, продающихся по два доллара за миллион. Никогда не возвращайтесь к ним, лучше уж на бумажке записывать, ей богу :)

Ну а мы тоже извлечем для себя урок, теперь будем прописывать в запрет на установку пароля даже те пароли, которых у нас никогда не было, но они попались нам в связке с вашим ящиком где-то в интернетах», вдруг вы решите к ним вернуться.

UPD: кстати, забыла сказать, что «хитрый пароль» у чувака был из букв, расположенных лесенкой на клавиатуре. Хитрости ему видимо добавляла единичка в конце.

UPD2: если у вас похожие аккаунты/ники на разных почтовых службах, а также в разных соц.сетях и службах знакомств, поверьте, злоумышленники умеют комбинировать: если украли базу, например, твиттера, где у вас ник vasya.petrov, то этот же пароль попробуют и к ящику vasya.petrov@mail.ru, vasya.petrov@gmail.com и т.п.

Автор: Виктория Федосеевко
11.08.2016, 16:42 25

© SmartBabr

НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР

3804

URL: <https://babr24.com/?ADE=270828>

Bytes: 5184 / 4810

Версия для печати

Скачать PDF

👍 Порекомендовать текст

Поделиться в соцсетях:

Также читайте эксклюзивную информацию в соцсетях:

- [Телеграм](#)

- [ВКонтакте](#)

Связаться с редакцией Бабра:

newsbabr@gmail.com



Автор текста: **Виктория Федосеенко**, журналист.

На сайте опубликовано **1274** текстов этого автора.

НАПИСАТЬ ГЛАВРЕДУ:

Телеграм: @babr24_link_bot
Эл.почта: newsbabr@gmail.com

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

[Прислать свою новость](#)

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: equatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

[Подробнее о размещении](#)

[Отказ от ответственности](#)

[Правила перепечаток](#)

[Соглашение о франчайзинге](#)

[Что такое Бабр24](#)

[Вакансии](#)

[Статистика сайта](#)

[Архив](#)

Календарь

Зеркала сайта