

1. Включите двухэтапную проверку для почты, платёжных и социальных аккаунтов: в первую очередь выбирайте подтверждение во всплывающем окне на телефоне, и лишь затем — код из СМС

Выгодность исходной версии: очень высокая

Доказательность А · исходная версия

для денег

бесплатно

мимоходом

без силы воли

Не зависит от страны

Оценки выше относятся к исходной версии; отдельная оценка российского варианта не проводилась.

Простыми словами

Двухэтапная проверка означает, что при входе, помимо пароля, нужно ещё раз подтвердить, что это действительно вы. Если на телефоне всплывает окно, а вы нажимаете кнопку подтверждения, это блокирует более 90% попыток кражи аккаунта через фишинг. Старые способы с ответами на вопросы «Откуда вы входили в прошлый раз?» или «Какой у вас резервный адрес электронной почты?» блокируют лишь около 10% таких попыток.

Затраты

Бесплатно. Настроить нужно один раз для каждого аккаунта, это займёт две-три минуты.

Выгода

Google проанализировал 350 тыс. реальных попыток кражи аккаунтов, также называемой захватом аккаунтов. Один вид проверки — с помощью устройства: например, на телефоне всплывает окно, в котором нужно нажать кнопку подтверждения, или нужно подключить аппаратный ключ безопасности. Этот вид проверки заблокировал «более 94% попыток захвата аккаунтов через фишинг и 100% автоматизированных попыток захвата». Фишинг — это когда вас обманом заставляют ввести пароль на поддельном сайте. Автоматизированные попытки — это когда программа массово пробует войти с утёртыми паролями. Другой вид проверки — с помощью ответов на вопросы: например, откуда вы входили в

прошлый раз или какой у вас резервный адрес электронной почты. Этот вид проверки «блокировал вплоть до всего 10% попыток захвата через фишинг и 73% автоматизированных попыток захвата»

Примечания

То же исследование показало, что такая проверка иногда не пускает в аккаунт и самого владельца. 52% настоящих пользователей не смогли войти с первой попытки, но в итоге 97% всё же вошли. Сначала включите эту функцию для почты, потому что пароль от большинства других аккаунтов можно восстановить через почту. Используйте коды подтверждения только сами. Какие последствия могут быть, если сообщать коды или проходить проверку по лицу за других, см. в разделе 8, пункте 45 (зачитывание кода подтверждения)

Источники

Источники исходной версии

1. Doerfler P, Thomas K, Marincenko M, et al. (2019). Evaluating Login Challenges as a Defense Against Account Takeover. The World Wide Web Conference (WWW '19).
doi.org/10.1145/3308558.3313481