«Извините, ошибка входа»

Алина, Москва

У меня был инстаграм, популярный, я получала приличный доход: 60 000 подписчиков, налаженные отношения с брендами, с аудиторией.

Однажды мне пришло 11 уведомлений о подозрительном входе в почту. Подумала, что это оповещение администрации почтовой системы, открыла последнее сообщение и увидела ссылку для подтверждения пароля. Перешла по ссылке, ввела свой пароль два раза и нажала кнопку «подтвердить». Через пару минут пришло уведомление о смене пароля в инстаграме. Письма из папки «Входящие» в почтовом ящике были перемещены в корзину, хотя я их не удаляла.

Я стала открывать все приложения, привязанные к почте, и поняла, что почти никуда не могу войти — у половины аккаунтов пароль был одинаковый. Мошенники все поменяли — пароль, адрес электронной почты и номер телефона, привязанные к аккаунту в инстаграме. Позже я получила письмо от взломщиков. За восстановление страницы они требовали 15 000 рублей немедленно, в противном случае — грозились удалить профиль.

Платить мошенникам не стала, не поверила, что они восстановят права входа.

Совет эксперта по противодействию мошенничеству:

Мошенники замаскировали свою ссылку под стандартное сообщение от почтового сервиса. Это частный случай фишинга — выманивания персональных данных пользователя в расчете на его невнимательность. Редкие люди вчитываются в те письма, которые им приходят от знакомых сервисов, и этим пользуются злоумышленники.

Взломать аккаунт в инстаграме мошенникам выгодно по нескольким причинам. Самый популярный способ заработать на похищенной учетной записи — потребовать вознаграждение за восстановление доступа к странице.

В других случаях взломщики используют страничку для рассылки спама и заработка в сети. Иногда такой вид мошенничества — способ отстранить бизнес-конкурента, вывести вперед аккаунт со схожей тематикой.

Как избежать мошенников?

- Регистрируйте аккаунт на проверенный почтовый ящик, который поддерживает двухфакторную аутентификацию — с помощью пароля и кода СМС.

- Не вводите адрес электронной почты на сомнительных сайтах: подозрительных интернет-магазинов, порталов, предлагающих с бесплатно скачать контент, интернет-казино.

- Не используйте одни и те же комбинации для авторизации разных страниц, регулярно обновляйте пароль. Используйте сложные пароли. Не отмечайте поле «Запомнить данные», если заходите на страницу с общедоступного компьютера. Иначе администрировать аккаунт смогут другие пользователи.

- Не переходите на другие сайты через профиль в инстаграме. Безопаснее скопировать ссылку и открыть ее в браузере.

- Свяжите аккаунты в инстаграме и на фейсбуке в настройках приложения. Это увеличит шансы восстановить доступ, если страницу взломают: даже если мошенники успели изменить пароль и почту, остается шанс пройти авторизацию через профиль в социальной сети.

- Не пользуйтесь программами накрутки подписчиков и лайков. Мошенники часто имитируют такие сервисы, запрашивают логин и пароль аккаунта, а затем похищают страницу.

- Если страницу уже взломали, сообщите о нарушении в справочный центр и обратитесь в службу техподдержки социальной сети. Будьте готовы отправить фотографии, подтверждающие личность, фото паспорта и персональные данные.