«Кто-то меняет ваш телефон на Госуслугах. Срочно скажите секретный код»

Светлана, Рязань

Неделю назад у меня чуть не увели аккаунт на Госуслугах. Самое обидное, что я поверила мошенникам и сама сообщила им данные для входа.

Позвонил мне якобы сотрудник службы безопасности Госуслуг. Сказал, что прямо в эту минуту кто-то пытается поменять номер телефона в моем личном кабинете. И если это делаю не я, то сейчас мне в СМС отправят код, который остановит операцию. Конечно, я его назвала.

«Безопасник» начал расспрашивать, не передавала ли я свои логин и пароль кому-то из знакомых, кто и где мог их подсмотреть. Потом сказал, что раз хакеры взломали мой аккаунт, то они могли получить доступ и к банковским счетам. Поэтому он соединит меня со специалистом Центробанка. Тут у меня в голове наконец щелкнуло, и я положила трубку: совсем недавно читала историю про мошенников, которые представляются сотрудниками ЦБ.

Тут же попыталась войти в свой кабинет на Госуслугах, но не получилось – пароль не подходил. Попробовала его восстановить. Портал потребовал ответ на какой-то контрольный вопрос.

Я точно помнила, что не устанавливала никаких вопросов. Сразу под строкой «Контрольный вопрос» была надпись «Технические работы», а затем уже поле для ответа. Подумала, может, просто какой-то сбой, и на всякий случай решила все-таки вбить ответ на контрольный вопрос, который всегда везде оставляю, – девичью фамилию матери. Попробовала – не сработало. Появилось сообщение, что мне нужно обратиться в МФЦ с паспортом и СНИЛС, чтобы восстановить доступ к аккаунту.

Я скорее побежала в МФЦ – к счастью, он недалеко от меня. Там мне помогли войти в личный кабинет на Госуслугах и посоветовали проверить, что взломщики делали в аккаунте, какую информацию

запрашивали. Выяснилось, что они успели заказать мою кредитную историю и справку 2-НДФЛ в налоговой.

Получается, мошенникам теперь известна масса информации обо мне. Чем это может грозить?

Совет эксперта по противодействию мошенничеству:

Из рассказа Светланы понятно, что у мошенников изначально было немало ее данных – не только имя и телефон, но и номер паспорта, ИНН или СНИЛС. Иначе они не смогли бы сменить пароль от ее аккаунта на «Госуслугах».

Вероятно, человек, который выдавал бы себя за сотрудника ЦБ, должен был убедить Светлану под какими-то предлогами перевести аферистам все свои деньги и вдобавок взять кредит. Ведь мошенники уже запросили ее кредитную историю и данные о доходах – так им проще понять, какую сумму стоит запрашивать, чтобы заявку точно одобрили. Либо аферист просто выведал бы у Светланы недостающие данные для входа в ее онлайн-банк и провернул бы все эти операции сам.

Светлана вовремя прервала разговор и не дала обманщикам дополнительной информации. Но опасность ей все еще грозит. Теперь у взломщиков есть и паспортные данные, и СНИЛС, и ИНН Светланы. Этих данных достаточно, чтобы попытаться взять онлайн-заем в микрофинансовой организации. Не исключено, что мошенники так и сделают. МФО усилили проверку заемщиков, но все же порядок идентификации клиентов там проще, чем в банках. Так что риск остается.

Если компания предлагает вам во что-то вложить деньги и при этом не заключает с вами договор, не связывайтесь с ней. Прежде чем передавать кому-то свои сбережения, нужно сначала тщательно изучить все документы.

Что делать, если вы оказались в подобной ситуации:

1.Никому и ни под каким предлогом не сообщайте секретные коды из уведомлений. Всегда внимательно читайте, что именно за код вам пришел, прежде чем его где-то вбивать.

2.Возможно, стоит перевыпустить банковские карты. Если мошенники знают реквизиты вашей карты, они могут попытаться сменить пароль от вашего онлайн-банка или просто обчистить ее.

3.Подайте в полицию заявление о взломе вашего аккаунта на «Госуслугах» (сохраните копию заявления и талон-уведомление о его приеме). Так вам будет проще доказать банку или МФО, что кредиты и займы брали не вы, если мошенникам все же удастся их оформить.

4.Периодически проверяйте свою кредитную историю. Если там обнаружатся чужие долги, нужно поскорее их оспорить.