Предупреждаем граждан о случаях мошенничества

Проблема кибер-мошенничества остается по-прежнему актуальной. Ежедневно значительное число граждан становится жертвами противоправных действий. Мошенники часто совершают преступные действия с помощью телефона, сети Интернет, удаленного доступа к персональным данным граждан и банковской карте. При этом преступники постоянно используют новые способы для обмана своих жертв. Так, в последнее время участились случаи мошенничества с аккаунтами пользователей на Интернет-портале «Госуслуги».

Мошенники чаще стали обманывать россиян от имени специалистов портала «Госуслуги». Речь идет о схеме, аналогичной получению доступа в онлайн-банки. Особой угрозе подвергаются люди пожилого возраста, у которых преступники пытаются получить информацию о размере пенсии, ее способе получения или доставки. Пытаются собрать сведения личного характера, о детях, месте работы, банковских вкладах. Мошенники могут рассылать на мобильные телефоны смс-сообщения с просьбой передать свои личные данные на указанный номер. Этого делать ни в коем случае нельзя.

Как себя обезопасить от мошенников.

Не перезванивайте на незнакомые номера, не переходите по ссылкам, если не уверены в отправителе сообщения. Не открывайте вложенные файлы в подозрительных сообщениях и не сообщайте свои персональные данные, в том числе информацию об имеющихся банковских картах. (Для сведения: персональные данные – это имя, фамилия, отчество, дата и год рождения, адрес, электронная почта, данные паспорта и других личных документов.)

Для безопасной работы с данными на Госуслугах:

• используйте уникальную связку логина и пароля.
• храните логин и пароль в безопасности.
• не передавайте кому-либо информацию для входа в ваш личный кабинет, приходящую от отправителя gosuslugi и номера 0919.
• используйте двухфакторную аутентификацию.
• включите уведомления от Госуслуг на электронную почту.
• добавьте в личном кабинете контрольный вопрос — его будут запрашивать при восстановлении доступа.
• не заходите в личный кабинет со случайных компьютеров, интернет-кафе или других непроверенных мест.

• используйте только лицензионное программное обеспечение.
• устанавливайте все необходимые обновления безопасности, рекомендуемые производителем программного обеспечения.
• устанавливайте и регулярно обновляйте лицензионное антивирусное программное обеспечение, регулярно проводите проверку на отсутствие вирусов.
• не загружайте программы и данные из непроверенных источников, не посещайте сайты сомнительного содержания.

Если вы стали жертвой мошенников, либо подозреваете, что можете ею стать, немедленно звоните по номеру 02, с мобильного телефона 102 или 112.

Помните: Если позвонивший представляется сотрудником правоохранительных органов и просит Вас снять деньги и перевести их на указанный им счет (все равно под каким предлогом), делать это ни в коем случае нельзя! Запомните: это – мошенники!

23 Января 2022

Адрес страницы: https://omsk.sledcom.ru/news/item/1649321