Мошенники начали воровать профили на Госуслугах с помощью СМС

Аферисты звонят пользователям от имени сотрудников портала «Госуслуги» и просят продиктовать код из СМС — якобы для активации или привязки QR-кода о вакцинации к профилю человека. Но на самом деле с помощью этого кода они меняют пароль для входа в личный кабинет на портале.

Получив доступ к чужому профилю, преступники смогут оформить кредиты на имя его владельца или продать персональные данные на черном рынке другим аферистам. О новой схеме мошенничества сообщила газета «Коммерсантъ».

Чтобы защитить свой профиль, соблюдайте меры безопасности:

- **Добавьте контрольный вопрос**. Система безопасности портала задаст этот вопрос, если вы забудете пароль и захотите его восстановить. А вот мошенники, не зная на него ответа, не смогут получить доступ к вашему аккаунту, даже если узнают код из СМС для смены пароля.
- **Установите дополнительную идентификацию с помощью СМС**. Код из сообщения нужно будет вводить каждый раз при входе в свой аккаунт.
  Контрольный вопрос и СМС-подтверждение можно настроить в разделе «Безопасность» своего профиля.
- **Держите данные в секрете.** Никому не сообщайте логин, пароль, кодовое слово, а также коды из СМС от Госуслуг. Мошенники могут звонить от имени портала и под различными предлогами выспрашивать эту информацию, однако настоящие сотрудники никогда так не делают.
-

Нередко аферисты присылают фишинговую ссылку на фальшивую страницу Госуслуг и просят там ввести конфиденциальные данные. Например, чтобы прикрепиться к поликлинике или получить денежную компенсацию.

Легенда может быть любой — никогда не переходите по ссылкам от незнакомцев и не выполняйте другие их инструкции. Настоящий адрес портала стоит закрепить в избранных, сохранить в списке нужных ссылок или каждый раз внимательно вводить его вручную.

Больше инструкций по защите своего аккаунта можно найти на портале «Госуслуги».

Подробнее о том, как противостоять киберпреступникам и социальным инженерам, читайте в статьях «Как защитить свои гаджеты от мошенников» и «Как быстро распознать мошенника».

Источник:
Официальный сайт Банка России
по финансовой грамотности
Fincult.info