Внимание мошенники !

Мошенники придумали новую схему обмана с помощью портала «Госуслуги».

Злоумышленники представляются сотрудниками портала «Госуслуги» и через QR-коды получают доступ к личному кабинету своих жертв. Согласно схеме, злоумышленники просят граждан продиктовать код из СМС-сообщения якобы для активации или привязки QR-кода к странице пользователя. Преступники инициируют по телефону восстановление пароля к учетной записи жертвы, чтобы впоследствии украсть его аккаунт. Затем они могут использовать портал «Госуслуги» для оформления кредитов или для других противоправных схем.

Что делать, если вам позвонили и предложили привязать QR-код к странице на Госуслугах:

- положите трубку и не сообщайте никаких данных;

- не отправляйте SMS с кодами, не меняйте пароль с помощью звонившего;

- сообщите о звонке в МВД и на горячую линию поддержки портала Госуслуг или через платформу обратной связи.

Как защитить аккаунт на «Госуслугах» от мошенников?

- включить двухфакторную аутентификацию, то есть вход на портал не только по логину и паролю, но и одноразовому СМС-коду.

- удалить банки, МФО и тому подобные организации из числа тех, у которых есть доступ к персональным данным с «Госуслуг».

- регулярно, раз в полгода-год, менять пароли. Не только на «Госуслугах», но и на других сервисах. Ключевой момент в паролях, по мнению эксперта, — это их длина. Нужно устанавливать как можно более длинные пароли — свыше 12–14 знаков. В них необязательно включать множество специальных символов и цифр, главное, чтобы это не было какое-то известное слово или очевидное сочетание имени-фамилии. Такой пароль подобрать практически невозможно.