

Как мошенники получают доступ к СИМ-карте (основные методы)?

1 Мошенники могут звонить или отправлять сообщения, выдавая себя за сотрудников мобильной связи. Они используют различные предлоги, такие как «у вас истекает срок действия договора» или «подозрительная операция», и просят назвать коды из СМС. Эти коды мошенники затем используют для доступа к учётным записям на различных ресурсах. Например: Госуслуги.

2 Мошенники приобретают старые СИМ-карты, которые были возвращены в продажу. Перед покупкой они проверяют, не привязан ли номер к важным ресурсам, используя слитые базы данных или вручную вводя номер на различных сайтах. После покупки номера мошенники используют его для восстановления доступа к учётным записям. В результате они могут оформлять кредиты, совершать покупки, открывать счета и проводить финансовые операции от имени жертвы.

3 Мошенники используют украденные личные данные, чтобы обратиться к оператору связи и запросить перевыпуск СИМ-карты.

4 Мошенники предлагают скачать «полезную» программу, антивирус. После загрузки такой программы на ваше устройство она начинает выполнять скрытые функции — крадёт информацию, включая коды из СМС-сообщений. Эти коды могут быть использованы для доступа к различным сервисам.

5 Мошенники просят вас набрать определённую комбинацию на телефоне с номером мошенника, чтобы переадресовать все звонки и СМС на его номер.

Рекомендации по защите личных данных

1 Открепление старого номера: после смены СИМ-карты обязательно открепите старый номер от портала «Госуслуги» и других сервисов.

2 Регулярная проверка учётных записей:

- постоянно проверяйте свои учётные записи на наличие подозрительной активности;
- при обнаружении странной активности немедленно измените пароли.

3 Регулярная смена паролей: меняйте пароли на своих учётных записях регулярно, используя сложные комбинации. Не используйте один и тот же пароль для разных сервисов.

4 Обратитесь к мобильному оператору: если вы перестали пользоваться СИМ-картой, обязательно расторгните соответствующий договор об оказании услуг связи.

5 Включение двухфакторной аутентификации: активируйте двухфакторную аутентификацию везде, где это возможно. Это обеспечит дополнительный уровень безопасности, требуя подтверждения входа с помощью СМС-кода, секретного кода или кода, отправляемого на электронную почту.

6 Используйте сервис «Сим-карты» на Госуслугах: проверьте, сколько абонентских номеров оформлено на ваше имя, и заблокируйте лишние номера.