Эксперт рассказала о росте числа кибератак с использованием подменной SIM-карты

В России участились случаи подмены сим-карт, что связано с ростом использования двухфакторной аутентификации и криптовалютных кошельков. Екатерина Едемская, инженер-аналитик компании «Газинформсервис», пояснила, что такие атаки позволяют злоумышленникам захватить полный контроль над мобильным номером жертвы, что даёт доступ ко всем связанным с ним сервисам. Этот метод стал популярным, особенно в последние годы, когда криптовалюты и двухфакторная аутентификация через смс приобрели широкое распространение.

Мошенники действуют в несколько этапов. Сначала они собирают информацию о жертве с помощью фальшивых сайтов, имитирующих страницы мобильных операторов, а также через телефонные звонки и сообщения, выдавая себя за сотрудников операторов связи. С помощью социальной инженерии злоумышленники пытаются выманить паспортные данные, имя и адрес. После этого они обращаются в салон связи или службу поддержки оператора, чтобы подменить сим-карту, предоставив поддельные документы или минимальные данные, которые могут убедить оператора в их подлинности.

Как только сим-карта заменена, мошенник получает доступ ко всем сообщениям, включая коды для двухфакторной аутентификации и подтверждения транзакций в банковских и криптовалютных приложениях. Это позволяет преступникам управлять счетами жертвы, выводить средства или читать конфиденциальную переписку. Едемская отметила, что процесс восстановления контроля над телефоном может занять от нескольких часов до нескольких дней, что делает такие атаки особенно опасными, ведь в это время жертва теряет доступ ко всем связанным с номером сервисам. Эксперт порекомендовала использовать альтернативные методы двухфакторной аутентификации, такие как приложения для генерации одноразовых кодов, которые не зависят от мобильной сети и обеспечивают большую безопасность.