

Мошенники научились красть сим-карты дистанционно, подделывая учётные записи и перевыпуская eSIM. Александр Дубровин, бизнес-партнёр компании edna, объясняет, что теперь злоумышленникам не нужно идти в офис оператора с поддельными документами. Достаточно скомпрометировать учётную запись человека у оператора связи и использовать телефон с поддержкой eSIM. Мошенник перевыпускает eSIM, и владелец теряет доступ к своему номеру.

Число таких случаев резко возросло, что связано с увеличением количества виртуальных операторов связи, которые подключают номера онлайн. Мошенники выпускают новые сим-карты с чужими номерами у виртуальных операторов. Также увеличились утечки персональных данных, и многие пользователи пренебрегают безопасностью, используя простые пароли или одинаковые пароли для разных сервисов.

Номер телефона стал важным средством идентификации. Получив доступ к номеру, мошенник может снять деньги со счетов или взять кредит. Чтобы защититься, эксперт советует использовать сложные, случайно сгенерированные пароли и двухфакторную аутентификацию. При получении сообщений о перевыпуске или блокировке сим-карты следует немедленно обращаться в техподдержку оператора.