**1.Телефонное мошенничество**

**от имени операторов**

**сотовой связи**

У телефонных мошенников новая схема: теперь они представляются сотовыми операторами. Звонят и сообщают, что с Вашего номера была подана заявка на смену оператора. Затем предлагают помощь и просят доступ в личный кабинет абонента. Телефонное мошенничество основано на социальной инженерии — наборе психологических методов для получения желаемого результата.

В 2024 году мошенники стали активнее использовать новую схему обмана, представляясь сотрудниками операторов мобильной связи.

Когда во время такого телефонного разговора человек получает СМС с кодом для входа в онлайн-кабинет своего сотового оператора, мошенники просят озвучить им этот код. Абоненту поступает звонок якобы от сотрудника службы поддержки или другого представителя мобильного оператора, который предлагает продлить договор сотовой связи или получить бонусы к праздникам, тем самым они пытаются получить доступ в личный кабинет абонента и выманить коды доступа к различным сервисам, включая мобильный банкинг.

Также используется предложение поменять тарифный план на более выгодный. Важно, что для изменения условий обслуживания нужно перейти на портал для предоставления услуг (в личный кабинет абонента) — авторизация пользователя происходит посредством кода из СМС-сообщения. Гражданин, не видя подвоха, соглашается и сообщает необходимую информацию, открывая доступ к персональным данным. Получив доступ, мошенники могут оформить кредит — многие операторы сотовой связи сейчас оказывают банковские услуги.

Также через личный кабинет они настраивают переадресацию СМС-сообщений и перехватывают информацию о платежах с банковской карты — потом эти данные можно использовать, чтобы списать деньги со счетов. Кроме того, они просят передать код из СМС для доступа к личному кабинету на Госуслугах. Подобные действия позволят аферистам оформить электронную сим-карту для дальнейшего управления сервисами различных банков от имени обманутого.

Опасность состоит в том, что в случае «удачной атаки», злоумышленник получает доступ к основному средству аутентификации клиента во всех сервисах, включая онлайн-банкинг любого банка или сервисов государственных услуг.

**2. Как обезопасить**

**себя от обмана?**

Оператор использует специальные механизмы, чтобы злоумышленники не звонили абонентам. Подозрительные вызовы выявляются с помощью аналитических алгоритмов и отсеиваются в автоматическом режиме или определяются, как спам звонок. Тем не менее, чтобы убедиться в том, что звонит представитель компании, нужно прекратить разговор и перезвонить на номер, указанный на официальном сайте оператора, от лица которого к Вам обращаются.

-------------------------------------------------

Отрывной талон

Памятка

«Телефонное мошенничество от

имени операторов сотовой связи»

Получателю социальных услуг:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Адрес проживания:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Банковские карты остаются главной целью преступников, которые используют и старые способы телефонного или интернет-мошенничества, и изобретают новые виды для кражи средств граждан.

Давно известны, но тем не менее срабатывают: звонок из службы безопасности банка, сообщение о выигрыше в лотерею, СМС о том, что карта заблокирована. Конечная цель мошенников всегда одна – узнать личные данные: номер карты, срок ее действия, код из трех цифр с обратной стороны карты или коды из СМС-сообщения, с помощью которых они входят в личный кабинет онлайн-банка жертвы и переводят деньги со счетов либо оформляют на человека кредит.

---------------------------------------------------

Отрывной талон

Памятку вручил, инструктаж провёл:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(должность, Ф.И.О.)

«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_г.

Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Памятку получил, с содержанием ознакомился:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Ф.И.О.)

«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_\_г

Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Информацию подготовил

специалист по социальной работе

организационно-методического

отделения Резник С.А.

Информация актуальна

на момент публикации

(апрель 2024 года)

**353740, ст. Ленинградская,**

**ул. Коммунальная, 42, каб. № 6а**

**8 (86145) 7 – 17 – 23**

**n.andriichenko@mtsr.krasnodar.ru**

[**www.leningradskiy-kcson.ru**](http://www.leningradskiy-kcson.ru)

**Государственное бюджетное учреждение социального обслуживания**

**Краснодарского края**

**«Ленинградский комплексный центр социального обслуживания населения»**

**Телефонное**

**мошенничество от**

**имени операторов**

**сотовой связи**

для получателей социальных услуг

**ст. Ленинградская**

**2024**