

«Киберпреступность: не стань жертвой мошенников!»

Несмотря на принимаемые правоохранительными органами меры, дистанционные хищения с использованием информационно-телекоммуникационных технологий стремительно набирают силу.

Мошенники умело используют всю доступную информацию и современные технологии, разбираются в психологии людей, вынуждая жертву раскрывать всю информацию о себе либо совершать те или иные действия, используют человеческие слабости и чувства в своих корыстных интересах.

В рамках повышения эффективности противодействия преступлениям, совершаемым с использованием информационных технологий (социальные сети, мессенджеры, звонки и смс, вредоносные ссылки и другое), отделением помощи семье и детям г. Геленджик разработаны информационные буклеты по данной тематике («Памятка для граждан о профилактике и предупреждении дистанционных преступлений в сфере информационных технологий»; «Советы для граждан по предупреждению киберпреступлений»). Также в целях противодействия киберпреступности Дальневосточным юридическим институтом (филиалом) Университета прокуратуры Российской Федерации при участии студенческого объединения «Киберволонтеры» разработаны следующие социальные видеоролики:

<https://disk.yandex.ru/i/WaxOnz8zzDpXQQ>

<https://disk.yandex.ru/i/VgQM6cWLVCat8g>

<https://disk.yandex.ru/i/I06gdo2qjz7PAQ>

<https://disk.yandex.ru/i/VieGq2HBF19bcg>

Просим ознакомиться с представленным в буклетах и видеороликах материалом в целях просвещения по данной тематике.

**ПАМЯТКА
ДЛЯ ГРАЖДАН
О профилактике и
предупреждении дистанционных
преступлений в сфере
информационных технологий**

Несмотря на борьбу с киберпреступностью, дистанционные хищения с использованием информационно-телекоммуникативных технологий стремительно набирают силу. Мошенники умело используют всю доступную информацию и современные технологии, разбираются в психологии людей, вынуждая жертву совершать те или иные действия в своих корыстных целях.

**Основные известные схемы
телефонного мошенничества:**

1. Случай с родственником.

Мошенник представляется родственником (знакомым) и взволнованным голосом по телефону сообщает, что задержан сотрудниками полиции за совершение преступления. Далее в разговор вступает якобы сотрудник полиции и уверенным голосом предлагает помощь, в обмен на вознаграждение.

2. Розыгрыш призов.

На телефон абонента приходит смс-сообщение, из которого следует, что он выиграл какой-то приз. Для уточнения всех деталей потенциальной жертве предлагается посетить какой-то определенный сайт и ознакомиться с условиями акции, либо позвонить по одному из указанных номеров.

3. SMS-просьба.

Абонент получает на телефон сообщение: «У меня проблемы, позвони по такому-то номеру, если номер не доступен, положи на него определенную сумму и перезвони».

4. Платный код.

Поступает звонок, якобы от сотрудника службы технической поддержки оператора мобильной связи, с предложением подключить новую эксклюзивную услугу или для перерегистрации во избежание отключения связи из-за технического сбоя, или для улучшения качества связи. Для этого абоненту предлагают набрать под диктовку код, который является комбинацией для осуществления мобильного перевода денежных средств со счета абонента злоумышленникам.

**5. Штрафные санкции
оператора.**

Злоумышленник представляется сотрудником службы технической поддержки оператора мобильной связи и сообщает, что абонент сменил тарифный план, не оповестив оператора (либо не внес своевременно оплату, либо воспользовался услугами роуминга) и, соответственно, ему необходимо оплатить штраф в определенном размере.

**6. Ошибочный перевод
средств.**

Абоненту поступает сообщение о поступлении средств на его счет, приведенных с помощью «мобильного перевода». Сразу после этого поступает звонок и злоумышленник сообщает, что он ошибочно перевел деньги на его счет, при этом просит вернуть деньги обратно. При этом на счет потенциальной жертвы никакие средства не поступают, однако жертва переводит злоумышленникам свои собственные средства. Кроме того, существуют такие номера, при осуществлении вызова на которые с телефона снимаются все средства.

7. Предложение получить доступ к sms-переписке и звонкам абонента.

Учитывая склонность некоторых людей «пошпионить» за близкими и знакомыми, злоумышленники предлагают за символическую плату получить доступ к переписке или контактам интересующего абонента. Когда потенциальная жертва вводит свои данные, либо совершает оплату за данную услугу, происходит списание всех доступных средств со счета или с номера телефона. А интересующая информация жертве так и не поступает.

8. Продажа на интернет-сайтах.

При звонке на телефон, размещенный на сайте (объявлений), злоумышленник просит пополнить счет его телефона или сообщить данные и номер карты для перевода на них денежных средств (для якобы оплаты или задатка за продаваемый товар). После сообщения этих данных происходит списание с них денежных средств.

9. Взлом аккаунта друга.

Взломав чужой аккаунт, злоумышленник пишет близким контактам сообщение с просьбой срочно помочь и перевести ему деньги. Люди не подозревают, когда им пишет чужой человек под видом родственника или друга, и, в попытке помочь близкому в беде, переводят свои денежные средства мошенникам.

10. Хищения с карт, подключенных к опции бесконтактных платежей.

Для проведения оплаты по карте (до 1000 рублей) достаточно приложить карту к терминалу. При этом количество транзакций не ограничено. Чтобы получить деньги потенциальной жертвы, мошеннику не нужно воровать карту, достаточно поднести устройство переносного терминала к сумке или карману, где находится карта.

11. Вишинг.

«Вишинг» - новый вид мошенничества, при котором злоумышленники под любым предлогом вынуждают потенциальную жертву предоставить конфиденциальную информацию о себе, которая в дальнейшем используется для доступа к денежным счетам жертвы.

ОТДЕЛЕНИЕ ПОМОЩИ СЕМЬЕ И ДЕТЯМ

ПАМЯТКА ДЛЯ ГРАЖДАН О профилактике и предупреждении дистанционных преступлений в сфере информационно- телекоммуникативных технологий



**ГКУ СО КК
«Новороссийский социально-
реабилитационный центр для
несовершеннолетних»**

г. Геленджик,
ул. Курзальная, 12
тел. 5-00-14

2024 год

**Советы для граждан
по предупреждению киберпреступлений**



ГКУ СО КК
«Новороссийский социально-реабилитационный центр для
несовершеннолетних»

г. Геленджик,
ул. Курзальная, 12
тел. 5-00-14

2024 год

**Советы для граждан по предупреждению
киберпреступлений:**

Чтобы не оказаться жертвой
мошенников необходимо знать
следующее:

- сотрудники любого банка никогда не просят сообщить данные вашей карты (номер карты, срок её действия, секретный код на оборотной стороне карты), так как у них однозначно имеются ваши данные;
- не при каких обстоятельствах не сообщать данные вашей банковской карты, а так же секретный код на оборотной стороне карты;
- хранить пин-код отдельно от карты, ни в коем случае не писать пин-код на самой банковской карте;
- не сообщать пин-код третьим лицам;
- остерегаться «телефонных» мошенников, которые пытаются ввести вас в заблуждение;
- лучше избегать телефонных разговоров с подозрительными людьми, которые

представляются сотрудниками банка, не бойтесь прервать разговор, просто кладите трубку;

– внимательно читайте СМС сообщения приходящие от банка;

– никогда и никому не сообщайте пароли, и секретные коды, которые приходят вам в СМС сообщении от банка;

– помните, что только мошенники спрашивают секретные пароли, которые приходят к вам в СМС сообщении от банка;

– сотрудники банка никогда не попросят вас пройти к банкомату;

– если вас попросили пройти с банковской картой к банкомату, то это очевидно мошенники;

– не покупайте в интернет – магазинах товар по явно заниженной стоимости, так как это очевидно мошенники;

– никогда не переводите денежные средства, если об этом вас просит сделать ваш знакомый в социальной сети, возможно мошенники взломали аккаунт, сначала свяжитесь с этим человеком и узнайте действительно ли он просит у вас деньги;

– в сети «Интернет» не переходите по ссылкам на неизвестные сайты;

– действуйте обдуманно, не торопливо, помните, что «Бесплатный сыр только в мышеловке».

ПОМНИТЕ: Своевременное обращение в правоохранительные органы может помочь другим людям не попасться на незаконные уловки телефонных мошенников.

Противостоять мошенникам возможно лишь повышенной внимательностью, здравомыслием и бдительностью.



Будьте бдительны и осмотрительны!