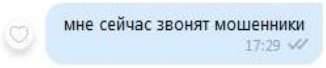
Меры по противодействию киберпреступлениям, профилактике их совершения, повышению цифровой грамотности населения.

Киберпреступления – это преступления, связанные с использованием компьютерной техники (преступления против информационной безопасности, хищения путем использования средств компьютерной техники, шантаж, вымогательство, изготовление и распространение порнографических материалов и т.д.).

За последнее время число киберпреступлений в мире увеличилось в огромное количество раз, мотивы и цели киберпреступников меняются с течением времени, а опасность совершаемых преступлений возрастает с каждым годом.

Все чаще мошенники для получения доступа к персональным данным, реквизитам банковских платежных карточек, паролям и другой конфиденциальной информации используют методы «социальной инженерии»: не взламывают устройства, а выманивают нужную информацию, используя ваши эмоции.

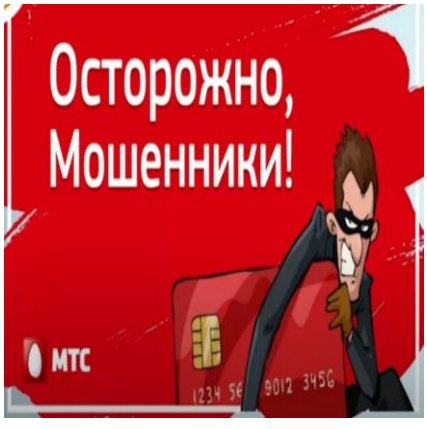


Основные формы мошенничества:

1. ***<u>«Звонок из Банка, компании МТС, А1»</u>*.**

Вам звонит незнакомое лицо. Номер входящего звонка очень похож на номер банка, компании МТС, А1, а звонящий представляется работником банка или же сотрудником компании МТС, А1).

Для реализации мошеннической схемы также используются мессенджеры (Viber, WhatsApp). Входящий звонок максимально закамуфлирован под звонок банка или компании МТС, А1: на экране может использоваться логотип банка, компании МТС, А1 (полностью или частично), а отображаемые номера телефона могут быть схожи, поэтому стоит быть особенно бдительным и обращать внимание на номера, а также на то, что через какой канал осуществляется звонок.



У мошенников есть возможность звонить с номеров, похожих на официальные номера банка, МТС, А1. Злоумышленники меняют цифры в номере, которые вы можете не заметить и просят у

вас конфиденциальные данные: логин и пароль от Интернет-банкинга, код из SMS от Банка, реквизиты карты (полный номер карты и срок ее действия, CVV- или CVC-код), а также идентификационный номер паспорта.

ВАЖНО! Никогда, никому и ни при каких обстоятельствах не сообщать реквизиты своих банковских счетов, банковских карт и идентификационный номер паспорта в том числе лицам, представившимся сотрудниками банка, компаний МТС, А1, правоохранительных органов, при отсутствии возможности достоверно убедиться, что эти люди те, за кого себя выдают. Сотрудники банковских учреждений, компании МТС, А1 никогда не используют для связи с клиентом мессенджеры (Viber? Telegram? WhatsApp).

Как мошенник пытается вас убедить.

· «*Мы звоним с официального номера, проверьте на сайте».*
· *«В целях конфиденциальности я включаю робота, который защитит ваши данные»* (вы слышите в трубке лёгкий шелест).
· Для убедительности он называет ваши персональные данные (имя, отчество, последние 4 цифры карты и др.) и просит перевести деньги *«на защищённый счет, который закреплён за персональным менеджером: это нужно для безопасности, а потом вы сможете вернуть деньги».*
· Или просит назвать ваши персональные данные или секретные коды из SMS роботу, при этом в трубке вы слышите музыку.
· Вам предлагают услуги страховки от мошеннических действий. Для ее оформления необходимо предоставить данные о карте, на которой находятся значительные денежные средства и SMS-код для подтверждения операции.

2) Мошеннические сообщения

Мошенники используют службы передачи сообщений и мессенджеры, такие как SMS, WhatsApp, Viber и другие, чтобы выманивать у людей деньги. Фишинг с использованием службы SMS даже получил название «смишинг». Существует множество мошеннических схем с использованием мессенджеров.

- Вы получаете SMS-сообщение о том, что вам пришла посылка, для получения которой необходимо подтвердить свою личность или оплатить стоимость доставки.
- Вместо ссылки мошенник может направить вам QR-код, который также хранит в себе ссылку на фишинговый сайт. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику.

- Вы получаете сообщение якобы от вашего банка о том, что ваш счет будет закрыт или ваша карта будет заблокирована, а на вас будет наложен штраф. Чтобы этого не случилось, вам нужно подтвердить свой аккаунт (разумеется, на поддельном веб-сайте).
- Вы получаете сообщение о крупном выигрыше, но, чтобы получить его, вы должны сообщить свои платежные реквизиты.

Как не попасться на удочку мошеннических сообщений.

Если организация, от имени которой пришло сообщение, раньше не связывалась с вами через мессенджер, это первый тревожный сигнал. Официальные организации не будут отправлять неожиданные сообщения через мессенджер с просьбой предоставить им личные или конфиденциальные данные. Проверьте, нет ли в сообщении орфографических или грамматических ошибок. Если сообщение выглядит непрофессионально – возможно, это признак онлайн-мошенничества. Если у вас возникли сомнения, не переходите по ссылкам и не сообщайте никакую персональную или финансовую информацию.

3) Поддельные интернет-магазины

Новейшие технологии позволяют создавать поддельные сайты интернет-магазинов, которые выглядят совсем как настоящие. Мошенники крадут логотипы и копируют дизайн страниц. На таких сайтах пользователям предлагают популярные бренды одежды, ювелирных изделий или электроники по низким ценам. Иногда пользователи получают оплаченный заказ, но чаще всего нет. В последнее время мошенники часто создают интернет-магазины в соцсетях. Такие магазины довольно быстро исчезают, чтобы вновь возродиться под другим названием.

Как распознать поддельный интернет-магазин: если какой-либо товар предлагают по невероятно низкой цене – это явный признак мошенничества. Еще один признак – если продавец настаивает на предоплате или оплате электронным, или телеграфным переводом.

Важно! Не переходите по подозрительным ссылкам. Для веб-версии Интернет-банкинга используйте только официальный сайт Банка, а для мобильной версии – только мобильное приложение, загруженное из официальных магазинов. Внимательно изучите сайт, на котором вводите личные данные. Обязательно проверьте наличие такого сайта в интернете.

Вриод начальника Горецкого РОВД
подполковник милиции С.В. Питяков