Министерство внутренних дел Российской Федерации

# Основные способы совершения преступниками мошеннических действий с использованием IT-технологий и рекомендации по их недопущению

Москва – 2022

«…Нужна последовательная, более результативная работа по всем видам преступлений, которые представляют угрозу для нашего общества. В том числе речь идёт о новых вызовах, связанных с проникновением криминала в сферу информационных технологий и телекоммуникаций. Количество преступлений в этой сфере ежегодно растёт. В результате действий кибермошенников урон несут отечественные компании. И, что вызывает особую остроту общественной реакции, с потерями средств и накоплений, с невосполнимым моральным ущербом сталкиваются наши граждане во всё большем и большем количестве. Жертвами преступников становятся пенсионеры, многодетные семьи, люди с ограниченными возможностями по здоровью. У преступников нет ничего святого, только бы деньги урвать …».

Президент Российской Федерации **Владимир Путин**

Из выступления на расширенном заседании коллегии МВД России по подведению итогов оперативно-служебной деятельности органов внутренних дел за 2021 год
17.02.2022

«В Российской Федерации с использованием IT-технологий по-прежнему совершается каждое четвертое преступление. Однако за три месяца текущего года* их количество заметно сократилось – на 8,5%. По мнению специалистов, это свидетельствует о том, что в данном процессе были массово задействованы кол-центры, расположенные на Украине, и обезвреженные в ходе специальной военной операции Вооружённых Сил Российской Федерации».

Министр внутренних дел Российской Федерации
генерал полиции Российской Федерации
**Владимир Колокольцев**

* За период с января по март 2022 года

Из выступления
на Совещании министров
внутренних дел
и общественной безопасности
государств – членов ШОС
18.08.2022

# СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Самым «действенным» способом мошенничества остаётся **социальная инженерия** – обман на доверии. Суть социальной инженерии состоит в том, что **злоумышленник вводит в заблуждение жертву** и та выполняет его инструкции, сама отдаёт ему деньги либо пароль от личного кабинета в онлайн-банке.

**Социальная инженерия**

Данный термин придуман ещё в начале 2000-х годов бывшим компьютерным хакером, признанным виновным в совершении различных компьютерных и коммуникационных преступлений, утверждавшим, что самое уязвимое место в кибербезопасности – человек.

Надо отметить, что характерной чертой современных правонарушителей является **беспринципность действий**. Мошенники с помощью психологического манипулирования заставляют людей делать то, что они делать не собирались, обманным путём выманивая у них последние сбережения, заставляя брать на себя кабальные кредитные обязательства.

Ключевым фактором, способствовавшим совершению указанных преступлений, является низкий уровень правовой и финансовой грамотности населения.

# ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

**Обман по телефону: «Меня задержали, но можно откупиться»**

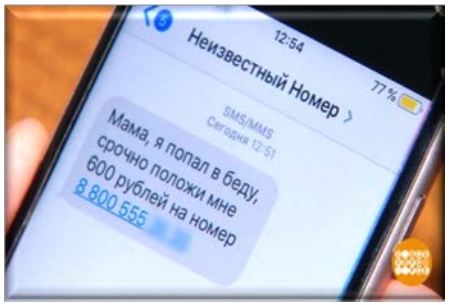
Вам звонят с незнакомого номера. Мошенник представляется родственником или знакомым и взволнованным голосом сообщает, что задержан сотрудниками полиции и обвинён в совершении того или иного преступления. Это может быть ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений и даже убийство.

Далее в разговор вступает якобы сотрудник полиции. Он уверенным тоном заявляет, что уже не раз помогал людям таким образом. Для решения вопроса необходима определённая сумма денег, которую следует привезти в оговоренное место или передать какому-либо человеку.


**Поступил сомнительный звонок ? Вам необходимо:**

- **прервать разговор и перезвонить тому, о ком идёт речь;**
- **если телефон отключён, связаться с его родственниками и друзьями для уточнения информации;**
- **если разговор происходит якобы с представителем правоохранительных органов, узнать, из какого он подразделения;**
- **набрать «02» и уточнить в дежурной части названного Вам подразделения, действительно ли родственник туда доставлен.**

## SMS, СООБЩЕНИЯ – ПРОСЬБА О ПОМОЩИ




Абонент получает сообщение на мобильный телефон: «У меня проблемы, кинь денег на этот номер. Мне не звони, перезвоню сам». Нередко добавляется обращение «мама», «друг» или другие.


Пожилым людям, детям и подросткам следует объяснить, что на сообщения с незнакомых номеров реагировать нельзя, это могут быть мошенники!

## ТЕЛЕФОННЫЙ НОМЕР – ГРАБИТЕЛЬ

Вам приходит сообщение с предложением перезвонить на указанный номер мобильного телефона. Просьба может быть обоснована любой причиной – помощь другу, проблемы со связью или с Вашей банковской картой и другие.

После набора номера Вас долго держат на линии. Когда это надоедает, Вы отключаетесь – и оказывается, что с Вашего счёта списаны крупные суммы.

НА САМОМ ДЕЛЕ:

Мошенники регистрируют сервис с платным звонком без предупреждения абонента о снятии платы за звонок.

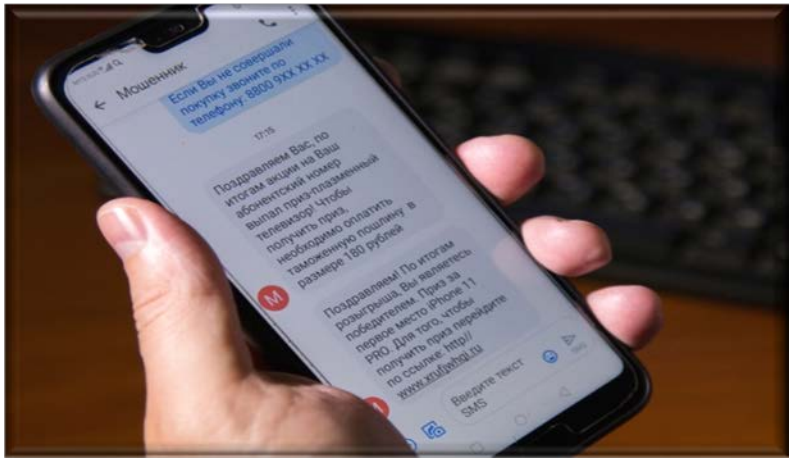
Будьте бдительны, совершая звонок по чужой просьбе!

**Единственный способ обезопасить себя от телефонных мошенников – это не звонить по незнакомым номерам!**

## «ВЫИГРЫШ» В ЛОТЕРЕЮ

Мошенники направляют сообщения с неизвестных номеров о выигрыше с просьбой осуществить перевод денежных средств для его получения либо вернуть якобы направленные (переведённые) ошибочно Вам денежные средства.

Если раньше мошенники звонили людям по телефону и рассказывали о выигрыше в лотерее, потом посылали такую информацию в SMS или по электронной почте, то сейчас им достаточно создать группу в социальной сети или мессенджере – «клиенты» придут сами.




Необходимо помнить, что человек не может выиграть приз, не участвуя в лотереях, родственники не будут отправлять сообщения с неизвестных номеров. Это обман. В этой связи не стоит отвечать на данные сообщения, а тем более отправлять информацию о своей банковской карте и переводить денежные средства!

## «ОШИБОЧНЫЙ» ПЕРЕВОД СРЕДСТВ

Вам приходит SMS-сообщение о поступлении средств на счёт, переведённых с помощью услуги «Мобильный перевод» либо с терминала оплаты услуг. Сразу после этого поступает звонок и Вам сообщают, что на Ваш счёт ошибочно переведены деньги и просят вернуть их обратно тем же «Мобильным переводом» либо перевести на «правильный» номер. Вы переводите, после чего такая же сумма списывается с Вашего счёта.

Если Вас просят перевести якобы ошибочно переведённую сумму, посоветуйте с чеком о проведённой операции обратиться в отделение банка.

Отговорка, что «чек потерян» скорее всего свидетельствует о том, что с Вами общается мошенник.

## ДЕНЬГИ ЗА ОНЛАЙН-ОПРОС

Мошенники предлагают ответить на несколько простых вопросов в Интернете, обещая выплатить баснословные деньги. Однако, чтобы их получить, нужно заплатить «комиссию». Естественно, после этого никакие деньги участнику опроса не приходят.



**Бесплатный адвокат**

Мошенники звонят гражданам и сообщают, что они стали потерпевшими по уголовному делу и им полагается адвокат. Его услуги якобы бесплатны, но нужно заплатить «госпошлину» – несколько тысяч рублей. Следует иметь в виду, что законом это не предусмотрено.

Если Вам предлагают просто так что-то очень выгодное, то скорее всего это обман. Не нужно верить таким предложениям.

## КОМПЕНСАЦИЯ ОТ «МИНЗДРАВА РОССИИ»

Мошенники в социальных сетях рассылают фейковую информацию, в которой сообщают гражданам, что им положены социальные выплаты, например, компенсация расходов на лекарства, а дальше предлагают пройти по указанной ссылке.

Зачастую злоумышленники пишут от первого лица: «Да, действительно вышел новый закон, я на себе проверил!». В доказательство прикладывают скриншоты с переводом денег от «Сбербанка». Их цель, чтобы человек перешёл по ссылке на сайт, в названии которого иногда даже используется слово «Минздрав», и ввёл свои персональные данные.

## КОМПЕНСАЦИЯ ОТ «МИНФИНА РОССИИ»

Обычно таким образом обманывают потерпевших от преступлений. Им звонят и говорят, что правительством выделена значительная компенсация для тех, кто пострадал от финансовых пирамид и других мошенничеств. Но, чтобы получить деньги, нужно якобы заплатить 1% от суммы компенсации.

Необходимо помнить, что мошенники рассылают подобные фейковые сообщения от различных государственных органов. Не поддавайтесь на их уловки!

# МОШЕННИЧЕСТВА, СВЯЗАННЫЕ С ПРОВЕДЕНИЕМ ЧАСТИЧНОЙ МОБИЛИЗАЦИИ И СПЕЦИАЛЬНОЙ ВОЕННОЙ ОПЕРАЦИИ

В настоящее время злоумышленники хорошо ориентируются в политической ситуации в стране, изобретая все новые предлоги для вымогательства денежных средств у граждан. Например, участились мошеннические действия, связанные с проведением частичной мобилизации, путем осуществления злоумышленниками звонков:

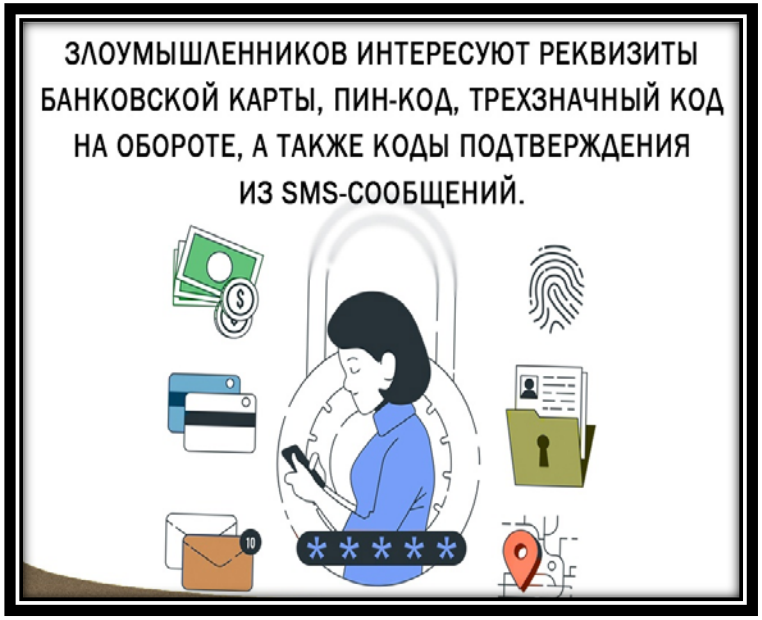
- от лиц, так называемых, известных «медийных персон» с предложением на платной основе услуг по обжалованию действий, связанных с нарушениями в ходе частной мобилизации;
- под видом сотрудников правоохранительных органов с угрозами лицам мужского пола уголовной ответственностью за уклонение от частичной мобилизации, одновременно предлагая за денежное вознаграждение «освобождение от призыва»;
- о предоставлении услуг по переводу из «первой очереди призыва» в «третью очередь призыва», оформлении отсрочки от призыва с использованием поддельных документов (справки о болезни, дипломы IT-специалиста и т.д.), оказание помощи в трудоустройстве по специальности, не подпадающей под частичную мобилизацию;
- под видом сотрудников правоохранительных органов с угрозами уголовной ответственностью за перевод денег в Украину и спонсирование террористических организаций;
- под видом участников волонтерских организаций о сборе денежных средств, якобы, для участников специальной военной операции и беженцев или «перевода» денежных средств в фонд «Вернись живым»;
- об «оказании помощи» в переезде граждан из Украины на территорию Российской Федерации за денежное вознаграждение.

В соответствии с законодательством Российской Федерации гражданин, воспользовавшийся указанными «услугами», подлежит привлечению к уголовной ответственности наравне с тем, кто данную «услугу» оказал.

## МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

Вам приходит сообщение о том, что Ваша банковская карта заблокирована. Предлагается бесплатно позвонить на определённый номер для получения подробной информации. Когда Вы это делаете, Вас просят сообщить номер карты, CVC-код или ПИН-код для её перерегистрации.

Для того, чтобы ограбить Вас, злоумышленникам нужны лишь реквизиты Вашей карты. Получив их, мошенники незамедлительно снимут деньги с Вашего счёта!




Необходимо помнить, что ни одна организация, включая банк, не вправе требовать Ваши CVC-код (трёхзначный код) или ПИН-код. Для того, чтобы проверить поступившую информацию о блокировке карты, следует самим позвонить в клиентскую службу поддержки банка (её телефон указан на оборотной стороне карты). Скорее всего, специалисты ответят, что Ваша карта продолжает обслуживаться банком.

## ПРАВИЛА БЕЗОПАСНОСТИ ПРИ ОБРАЩЕНИИ С БАНКОВСКИМИ КАРТАМИ

**Нельзя:**

- хранить ПИН-код рядом с картой, записывать его на бумаге;
- прибегать к помощи третьих лиц при проведении операций с банковской картой в банкоматах;
- позволять посторонним лицам использовать Вашу пластиковую карту.

# ФИШИНГ

Вид интернет-мошенничества, цель которого – получить Ваши персональные данные, получил название **фишинг** (от англ. fishing – рыбная ловля, выуживание).

Злоумышленники рассылают электронные письма от имени банков, платёжных систем, маркетплейсов и сервисов. Пользователю предлагается зайти на интернет-ресурс – точную копию настоящего сайта организации, которой человек склонен доверять.

Для дальнейшей возможности использовать свою пластиковую карту Вас просят указать её CVC-код и другие данные. Впоследствии эти данные используются для хищения денежных средств, содержащихся на Вашем счёте.

Фишинг используется мошенниками также на сайтах знакомств, поиска работы, консультационных услуг и т.д.

**Следует помнить:**

- банки и платёжные системы никогда не присылают писем и не звонят на телефоны граждан с просьбой о предоставлении своих данных;
- сотрудники банка располагают достаточной информацией о своих клиентах;
- сотрудники банка могут у Вас спросить кодовое слово в том случае, если Вы им сами позвонили.

Если звонят «из банка», то попросите «сотрудника» набрать Вам через пять минут. Прервав разговор с незнакомцем, позвоните сами в свой банк по номеру, который указан на Вашей карте, и поговорите с реальной службой поддержки банка.

## ВРЕДОНОСНЫЕ ПРОГРАММЫ И ТАКТИКА БОРЬБЫ С НИМИ

Интернет называют «миром новых возможностей». Но тем, кто только пришёл в этот мир, следует вести себя осторожно и строго следовать правилам поведения в Сети. Как и в реальном мире, в Интернете действует множество мошенников и просто хулиганов, которые создают и распространяют вредоносные программы.

**Вредоносные программы** – любое программное обеспечение, которое предназначено для скрытного (несанкционированного) доступа к персональному компьютеру с целью хищения конфиденциальных данных, а также для нанесения ущерба, связанного с его использованием.

Все вредоносные программы нередко называют одним общим словом «вирусы». Их можно разделить на три группы: компьютерные вирусы, сетевые черви, троянские программы.

## ОБЩИЕ РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОЙ РАБОТЫ В СЕТИ ИНТЕРНЕТ

- установите антивирусное программное обеспечение с самыми последними обновлениями антивирусной базы;
- регулярно обновляйте: антивирусные программы либо разрешайте автоматическое обновление при запросе программы, пользовательское программное обеспечение для работы в сети, такое как интернет-браузер, почтовые программы;
- не сохраняйте без предварительной проверки антивирусной программой файлы, полученные из ненадежных источников – скачанные с неизвестных веб-сайтов, присланные по электронной почте;
- по возможности, не сохраняйте в системе пароли и периодически меняйте их.