



## Информационно - справочные материалы, направленные на противодействие киберпреступности, повышение уровня осведомленности и киберграмотности граждан.

Материалы содержат основные схемы обмана населения, применяемые преступниками при совершении мошеннических действий, с использованием информационно - телекоммуникационных технологий.

Задача выступающих проинформировать граждан об известных уловках мошенников, выработать принципы и правила безопасного поведения в сети Интернет, а также сформировать навыки противодействия «телефонному мошенничеству».

Следует донести до населения, что на первоначальном этапе злоумышленники собирают персональную информацию о своих потенциальных жертвах, затем используют различные предлоги для контакта с ними. Приемы мошеннических схем основаны на неожиданности, напористости, запугивании, требовании немедленного принятия решения, имитации заботы. Мошенники в свои изощренные схемы включают психологическое давление и манипуляции, выводят человека из равновесия, приводят его в состояние страха, стресса, либо же завоевывают его доверие, демонстрируют сочувствие, налаживают эмоциональный контакт.

### Основные схемы обмана населения:

#### «Безопасные ячейки», «Безопасный счет»

Мошенники представляются работниками банка или сотрудниками правоохранительных органов и сообщают, что со счетов жертвы неизвестные пытаются похитить накопления. Для сохранения сбережений они просят перевести финансы на «специальный защищенный счет». Поверив аферистам, граждане лишаются всех денег и оформляют кредиты. На данный момент это самый распространенный вид мошенничества.

#### Звонок от иных «ведомств» и «организаций» (налоговая служба, страховые компании, службы ЖКХ, управляющие компании, риелторы, Госуслуги, Социальный фонд России и др.)

**Звонок от «представителя Госуслуг»:** мошенники сообщают, что на имя гражданина пришло электронное письмо и что необходимо назвать код из СМС, чтобы оно отразилось в личном кабинете на Госуслугах. Получив от человека СМС-код, злоумышленники получают доступ к аккаунту Госуслуг. В личном кабинете Госуслуг мошенники получают всю информацию о доходах, транспортных средствах, квартирах, налогах и кредитной истории.

**Звонок из «пенсионного фонда»:** лжесотрудник, обращаясь по имени отчеству к человеку, сообщает, что гражданину положены дополнительные выплаты, компенсации от государства или какого-нибудь фонда, либо о переплате средств. Убеждает человека, что для получения этой выплаты никуда ходить не надо - все деньги переведут на карту, необходимо только продиктовать все ее реквизиты, в том числе код с обратной стороны.

**Звонок из «Центробанка»:** лжесотрудник предлагает человеку установить на телефон приложение «Банкноты Банка России» для проверки подлинности 5-тысячной купюры. Вместе с приложением скачивается вредоносная программа, которая дает доступ к личному кабинету человека.

**Звонок из «поликлиники», «аптеки», «медицинского центра»:** мошенники преподносят информацию о проблемах со здоровьем гражданина и сообщают ему о появлении дефицитного и дорогого лекарства по специальной цене, которое надо срочно выкупить. Злоумышленники объясняют, что человек платит полную стоимость, а разницу в цене по скидке вернут ему на карту, реквизиты которой необходимо сообщить звонящему.

**Звонок от «оператора сотовой связи»:** злоумышленники сообщают об истечении срока действия сим- карты, договора об оказании услуг связи или о нарушении условий договора в связи с передачей номера другому оператору и предлагают решить проблему с использованием личных кабинетов Госуслуг. В процессе разговора гражданину поступает сообщение с кодом, сообщив его, предоставляет доступ к своему личному кабинету. Далее мошенники направляют заявки в кредитное учреждение на предоставление денежных средств, впоследствии полученные денежные средства переводят на подконтрольные счета.

#### Звонок от неизвестного лица о покупке или продаже товара/услуги

Человеку поступает звонок по объявлению, данному в Интернете. Мошенник - «потенциальный покупатель» соглашается на покупку и просит сообщить номер, срок действия и СУУ-код карты и после этого сообщить СМС-код банка о проведенной операции. Если мошеннику не удастся получить весь набор информации, то недостающие данные восполняются квалифицированными хакерами. В результате счет банковской карты не пополняется, а опустошается путем перевода наличности на некий электронный кошелек, который немедленно исчезает из сети после вывода средств с него.

#### Легкий заработок или же выигрыш крупной суммы

Человеку поступает звонок от якобы ведущего популярной радиостанции, который поздравляет с крупным выигрышем в лотерею, организованной радиостанцией или оператором мобильной связи. Мошенник убеждает в том, что для получения приза необходимо в течение минуты дозвониться на радиостанцию по указанному номеру телефона. Перезвонившему абоненту отвечает сотрудник «призового отдела» и грамотно убеждает в «честности» акции, просит представиться и назвать год рождения, подробно объясняет условия получения приза, причем для его получения требуется осуществить «незначительный» предварительный перевод денежных средств или предоставить персональные данные, данные карты, полученный код из СМС.

#### «Ваш родственник попал в беду»

Человеку (матери, отцу, бабушке) поступает звонок о попавшем в беду родственнике от имени правоохранительных органов или медицинских учреждений. Это может быть сообщение о ДТП, хранении оружия или наркотиков, нанесении тяжких телесных повреждений, убийстве. Лжесотрудник полиции по телефону уверенным тоном сообщает, что в данной ситуации можно помочь родственнику, но для решения вопроса (закрытия дела) необходима определенная сумма денег, которую следует привезти в определенное место или передать определенному человеку. После получения денежных средств «курьер» переводит полученную от потерпевших сумму на банковский счет или счет мобильного телефона.

#### Фишинговые атаки

Злоумышленники подделывают популярные сайты (к примеру, Госуслуги), а также подделывают сайты известных магазинов, маркетплейсов, туристических компаний, авиакомпаний и др. Имитируя Интернет-ресурсы популярных компаний, мошенники рассчитывают, что пользователи не заметят подделку и оставят на поддельной фальшивой странице личные или финансовые данные, логин и пароль, контактные сведения (номер телефона и электронную почту), а также оплатят покупку путевок, авиабилетов и иных услуг.

#### Распространение «Арк» файла

В мессенджере от неизвестных абонентских номеров, либо от имени знакомых направляются сообщения, имеющие файлы с расширением «арк», которые содержат вредоносные программы по сбору персональных данных, а также программы удаленного доступа, позволяющие управлять смартфоном, включая банковские онлайн предложения.

#### Правила защиты от мошенничества:

- 1. Не переводите деньги незнакомцам. Запомните! Самый безопасный счет — это тот, который открыт в банке. Перевод денег на «безопасный счет», «гарантийный депозит» — это обман.**
- 2. Никогда и ни при каких обстоятельствах не передавайте персональные данные** (пароли, пин-коды, данные паспортов или номера карт) третьим лицам.
- 3. Не сообщайте никому три цифры с обратной стороны карты, пин-код и коды, приходящие на телефон** — это конфиденциальная информация, предназначена только для вас. Сообщите их кому-либо - можете лишиться денег.
- 4. Не доверяйте подозрительным звонкам и сообщениям.** Сотрудники банков, правоохранительных органов никогда не интересуются вашими денежными средствами, при поступлении таких звонков просто положите трубку.
- 5. Никогда не скачивайте приложения по указанию неизвестных вам лиц**, а также из непроверенных источников в сети Интернет. Мошенники могут отправить подозрительные файлы, которые содержат вредоносный код. Клик по ссылке может взломать ваш телефон с личной информацией.
- 6. Будьте осторожны при совершении онлайн - покупок.** Используйте официальные интернет-магазины. Проверяйте надежность продавца, читайте отзывы других покупателей, используйте защищенные платежные системы.
- 7. Блокируйте подозрительные и рекламные номера.**
- 8. Договоритесь с родственниками и близкими о создании контрольного вопроса (слова), чтобы при звонке или смс-сообщении удостовериться, что звонит не мошенник.**
- 9. Оповещайте о мошенничестве.** Если вы стали жертвой мошенников, обратитесь в полицию и оповестите банк.

Дополнительная информация и видеоматериалы размещены на официальном сайте МВД России в разделе «Памятка для граждан» в подразделе «Социальные видеоролики» [https://мвд.рф/Videoarhiv/Socialnaja\\_reklama](https://мвд.рф/Videoarhiv/Socialnaja_reklama) - а также в Telegram-канале УБК МВД России «Вестник Киберполиции России» [https://t.me/cvberpolice\\_rus](https://t.me/cvberpolice_rus).

Кроме того, считаем возможным с привлечением сотрудников подразделений по противодействию экстремизму территориальных органов МВД России рассказать участникам мероприятий о методах вовлечения граждан в мошеннические схемы и деструктивную деятельность, направленную на разрушение объектов инфраструктуры с разъяснением ответственности, предусмотренной законодательством Российской Федерации за совершение диверсий.