БЕСЕДЫ с сотрудниками по киберпреступности

Киберпреступность растет с большой скоростью, признают в правоохранительных органах России.

Сотрудники Управления по противодействию киберпреступности МВД России составили небольшие информационные беседы в которых можно узнать о многих актуальных мошеннических схемах, откуда может исходить угроза и как ей противостоять.

Мошенники существовали всегда. Они умудряются похищать средства и ценности самыми разнообразными способами. Информатизация привела к появлению нового вида злодеев — кибермошенников.

Кибермошенничество — это один из видов преступлений в Интернете, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя.

Беседа1 "Ваш номер нужно подтвердить"
Беседа2 Беседа 2. "Предложения от лжеброкеров"
Беседа 3. "Вам предлагают выгодную работу"
Беседа 4. "Друг просит о помощи"
Беседа 5. "Оплата услуг по фейковому QR-коду"
Беседа 6. "Звонки из банка"
Беседа 7. "Представляются госслужащими"

Беседа 1. "Ваш номер нужно подтвердить"

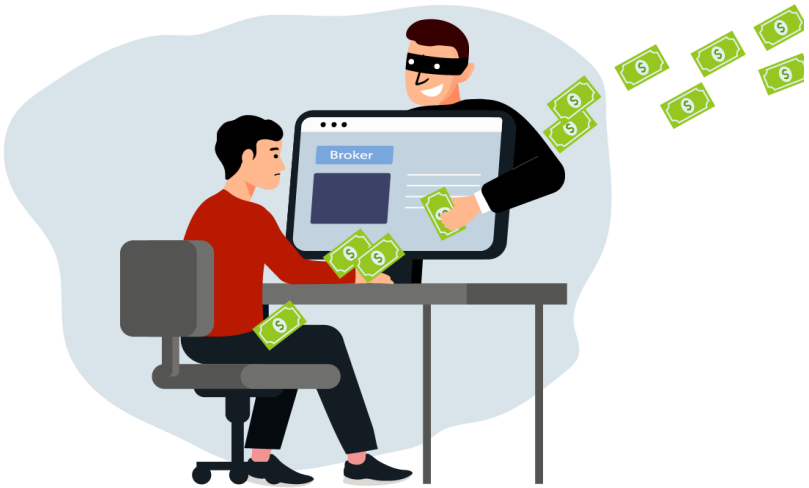
Простейший обман, который чаще всего срабатывает. Идет звонок якобы от оператора сотовой связи. Мошенники пугают, что действующий договор на оказание услуг связи заканчивается и его необходимо продлить, иначе номер передадут другому абоненту. Идти никуда не нужно, все можно сделать по телефону, уверяет собеседник. Достаточно продиктовать код из смс. На самом деле цель одна — получить доступ к аккаунту человека на Госуслугах.

Следующий шаг — перейти по присланной ссылке, где нужно ввести еще один код. Таким образом, человек не продлевает договор, который на самом деле является бессрочным, а предоставляет данные для входа в личный кабинет на портале «Госуслуги» и всю информацию о себе, которая там хранится.

Есть и другая цель, которую преследуют мошенники, представляясь оператором связи. Тот же звонок, но теперь с предложением по смене тарифного плана, подключением новых опций либо замены sim-карты. Чтобы это сделать, абонента просят продиктовать код из смс. С помощью этого кода злоумышленник получает доступ к личному кабинету пользователя на сайте оператора мобильной связи. А уже там он настраивает переадресацию сообщений и звонков с номера жертвы на свой. Это делается для того, чтобы в дальнейшем подтверждать разного рода операции: вывод средств с банковских карт абонента, оформление на него кредита и т.д..

Вы можете обновить персональные данные, обратившись за услугой лично, — в офисе оператора связи или в личном кабинете на его официальном портале (но не по ссылке из смс). Не называйте никаких данных незнакомым по телефону. Если сомневаетесь, позвоните оператору связи по номеру, размещенному на официальном сайте.

Беседа 2. "Предложения от лжеброкеров"



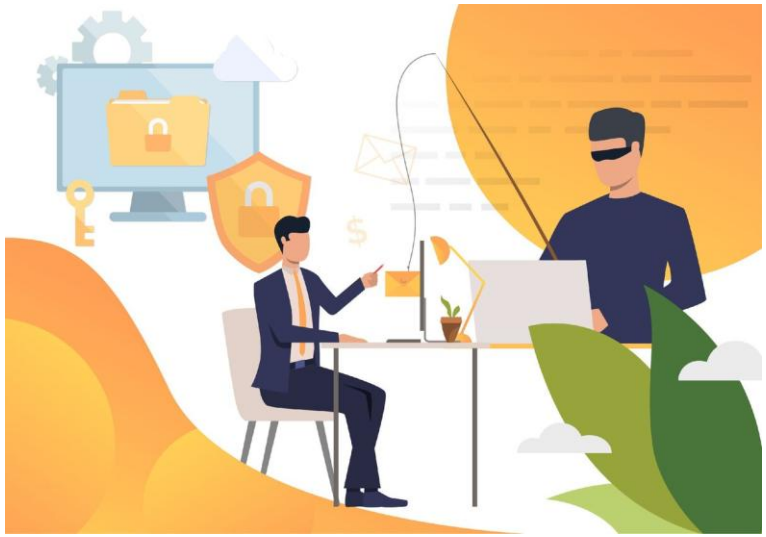
Аферисты предлагают вам выгодно вложить свои средства, обещая процент гораздо выше, чем у банков. С потенциальными инвесторами они связываются через социальные сети или звонят им под видом сотрудников известных инвестиционных компаний. Предложение заманчивое: нужно лишь открыть «брокерский» счёт и инвестировать от 10 тысяч рублей. Доход — не меньше миллиона. Для открытия такого счёта мошенники требуют установить приложение. Как только у «инвестора» возникает желание вывести деньги со счета, начинаются проблемы. Лжеброкеры говорят, что сделать это сложно. Нужно пополнить счёт еще раз на определенную сумму, оплатить «страховку». Или ежедневное размещение валюты в «европейской ячейке» либо найти поручителя, чтобы можно было «обналичить» средства. В итоге инвестор теряет свои деньги, а заодно и надежду на будущие миллионы.

Вариант этой же мошеннической схемы — участие в уникальном инвестиционном онлайн-проекте известного банка. Завлекают при помощи писем на электронную почту.

После вам предложат пройти опрос: указать заработок, предпочитаемый способ хранения средств и контактные данные для связи с представителем организации, а также дадут доступ к специальному приложению. А уже там понадобится ввести данные своей банковской карты — с нее аферисты потом и спишут деньги.

Как отличить мошенников от реальных брокеров? Проверьте сайт инвесткомпании или брокера. Обратите внимание на реквизиты и наличие лицензии Банка России. Откажитесь от услуг компании или её представителей, если они просят перевести деньги за услуги на карту физического лица, либо через электронный кошелек.

Беседа 3. "Вам предлагают выгодную работу"



Аферисты размещают лжевакансии на популярных сайтах объявлений. Зарплата привлекательная, условия работы заманчивые. Но нужно пройти собеседование с будущим работодателем, и мошенники предлагают сделать это онлайн по видеозвонку.

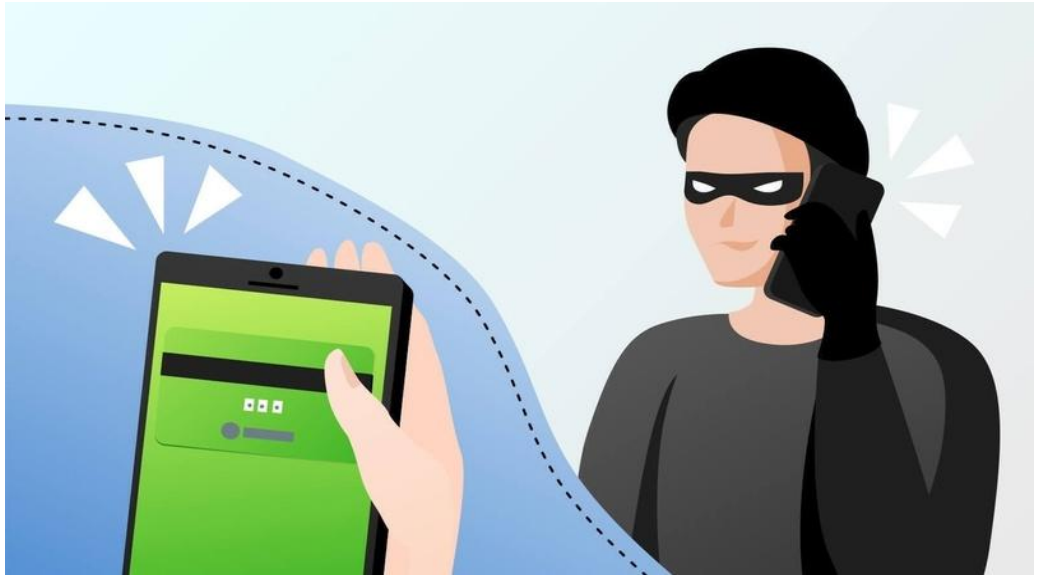
Собеседование с будущим работодателем — волнительная процедура. Во время онлайн-встречи мошенники пользуются растерянностью соискателей и крадут личные данные. Один из её пунктов — номер карты и другие финансовые данные. Такая информация им нужна якобы для перечисления зарплаты в будущем. Чтобы ничего не пропустить, они включают запись экрана. Некоторые мошенники просят указать информацию по нескольким банковским картам, если какую-то якобы не примет бухгалтерия. Понятно, что вместо пополнений с банковской карты соискателя в будущем происходят списания, а ни о какой работе речи не идёт.

Находясь в поиске работы, можно не только потерять деньги, но и нарушить закон, став дроппером. В последнее время именно этот мошеннический сценарий становится популярным, а его жертвами становятся студенты и пенсионеры.

Дропперы — подставные лица, которые задействованы в нелегальных схемах по выводу средств с банковских карт. Часто человек даже не осознает, что вовлечен в преступную схему. В

Чего нельзя делать при трудоустройстве онлайн? Внимательно изучайте предложение от будущего работодателя и отзывы о нём. Не верьте обещаниям лёгкого заработка с минимальной затратой собственного времени. При общении сохраняйте холодную голову, не поддавайтесь эмоциям, а главное — следите за данными, доступ к которым просит предоставить работодатель.

Беседа 4. "Друг просит о помощи"

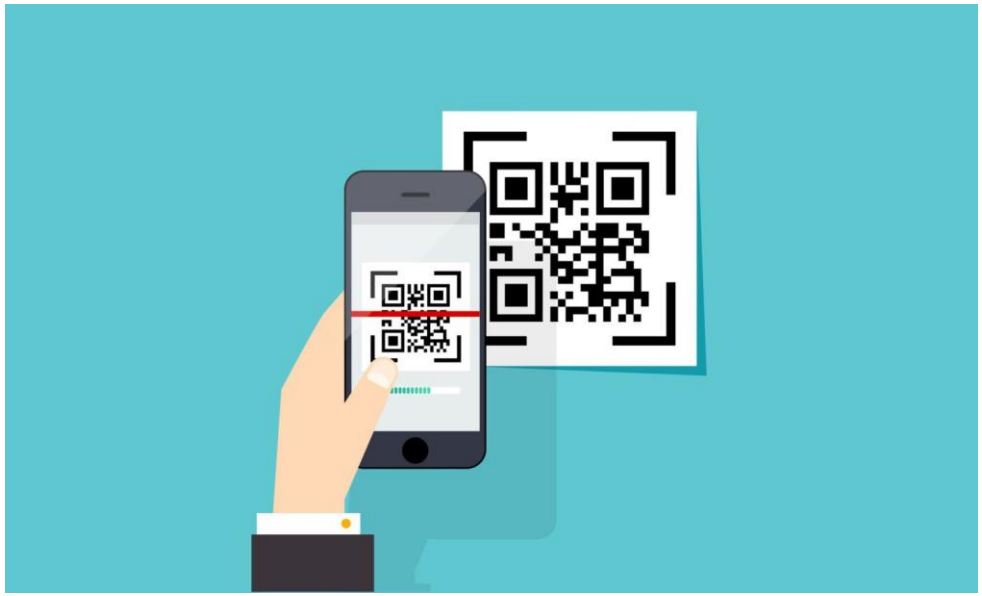


Старая, но рабочая схема мошенников. Несмотря на все предупреждения, жители снова и снова попадаются на эту уловку злоумышленников. На сотовые и стационарные телефоны граждан поступают звонки, и неизвестный на другом конце провода представляется кем-либо из родственников и сообщает, что попал в дорожно-транспортное происшествие, далее связь прерывается. Следом звонят якобы сотрудники правоохранительных органов и поясняют, что родственник потерпевших является виновником аварии и теперь для возмещения причиненного материального ущерба, воизбежания уголовной ответственности необходимо заплатить определенную сумму, а также указывают, кому требуется передать деньги. Опасаясь за своих близких, доверчивые граждане отдают деньги незнакомцам. Гражданам необходимо запомнить, что сотрудники правоохранительных органов не требуют вознаграждения за разрешение проблем граждан. За подобные действия в Уголовном кодексе Российской Федерации предусмотрена ответственность по статье 290 "Получение взятки".

Существует и другой сценарий — просьба проголосовать за детей в конкурсе. За ссылкой для голосования, которую мошенники отправляют со взломанного аккаунта владельца, скрыт вирус, который откроет им доступ к вашему гаджету.

Как понять, что родственник фальшивый. Не переходите по неизвестным ссылкам, даже если получили их от близких или знакомых. Договоритесь с родственниками о пароле или секретном вопросе, который нужно назвать, если разговор кажется подозрительным.

Беседа 5. "Оплата услуг по фейковому QR-коду"



Сегодня, чтобы получить какую-либо услугу или оплатить товар, достаточно навести камеру на QR-код. Например, им можно воспользоваться, чтобы взять в аренду самокат или портативное зарядное устройство для гаджета. Правда, вместо прогулки с ветерком и заряженного аккумулятора телефона можно получить пустой банковский счет.

Практически все современные телефоны могут считывать QR-коды без отдельного приложения – достаточно открыть камеру. То же самое касается и оплаты. При переходе по ссылке открывается банковское приложение, где нужно подтвердить платеж.

Аферисты разрабатывают QR-коды, которые ведут не на официальный сайт сервиса, а на поддельный ресурс, через который они крадут деньги и данные карты. Чтобы не стать жертвой обмана, необходимо оплачивайте услугу только через официальное приложение сервиса, а не через камеру гаджета.

Бывают случаи, когда преступники наклеивают поверх официального QR-кода свой, отсканировав код, деньги уходят на счет мошенников.

Как платить, чтобы не потерять деньги Оплачивайте услугу только через официальное приложение сервиса, а не через камеру гаджета.

Беседа 6. "Звонки из банка"

Мошенники представляются сотрудниками банка и сообщают, что кто-то пытается украсть с вашей карты деньги. Чтобы остановить преступление, они просят сообщить им полные реквизиты карты или дать доступ в личный кабинет. Этого делать нельзя. Что делать Обратите внимание Никогда не сообщайте по телефону незнакомцам cvc-код – трехзначный номер на обороте кредитной карты. Эта информация нужна для того, чтобы вывести деньги с карты или безналичным способом Проверяйте номер, с которого вам звонят. Часто преступники звонят с телефонных номеров, похожих на номера банков – с кодами 495, 499, 8 800. Не сообщайте никому данные ваших кредитных карт: номер, срок действия и cvc-код. В банке не станут просить производить какие-либо действия вне отделения банка. Блокировать карту без заявления клиента сотрудники тоже не будут. Из банка могут позвонить только с предложением какой-либо услуги или просьбой пройти опрос. Если вам позвонили мошенники, не вступайте с ними в переговоры, не реагируйте на угрозы, что сейчас с вашей карты снимут деньги. Их задача – вывести вас из равновесия. Сразу сообщите, что вы сами перезвоните в свой банк или посетите его лично, и повесьте трубку. После этого позвоните в банк по телефону, который указан на официальном сайте, и сообщите о подозрительном звонке, назовите номер телефона, с которого звонили мошенники.

Как проверить звонок из банка? Пользуйтесь только официальными ресурсами финансовых организаций. Если вам звонят сотрудники банка и разговор с ними кажется подозрительным, перезвоните на официальный номер, размещённый на сайте финансовой организации. Там же вы можете скачать официальные банковские приложения.

Беседа 7. "Представляются госслужащими"

Часто мошенники звонят или пишут человеку якобы от лица сотрудников ФСБ, налоговой, портала «Госуслуги». Самая распространенная уловка — предложение получить какую-либо госвыплату. Схема классическая: вы нам данные карты, мы вам — деньги.

Есть и другой сценарий. Например, звонок от следователя или Росфинмониторинга с угрозой блокировки счёта, по которому якобы зафиксированы сомнительные операции. Чтобы этого избежать, мошенники требуют оплатить штраф.

Что следует сделать: не верить таким звонкам вообще. Поскольку ведомства не наделены полномочиями по аресту денежных средств и никогда не оказывают платных услуг по телефону или в мессенджерах.

Если вы стали жертвой киберпреступников, обязательно нужно сообщить об этом в полицию. Даже если вам кажется, что это незначительное мошенничество, вполне вероятно, что вы поможете обезвредить профессиональную группу хакеров. В конце концов, борьба с киберпреступностью – это дело каждого!