**Типовая лекция**
**по профилактике преступлений в сфере информационно-телекоммуникационных технологий.**

На территории Оренбургской области правоохранительными органами все чаще регистрируются факты совершения хищений денежных средств с лицевых счетов граждан с использованием современных информационно-телекоммуникационных технологий. Потерпевшими становятся жители региона различных возрастных групп. Преступники при совершении хищений постоянно совершенствуются, придумывая новые способы, при этом активно используют Интернет-ресурсы, торговые площадки, возможности цифровой телефонии.

Чтобы не попасть на уловки мошенников необходимо каждому знать, каким образом совершаются преступления и что ни в коем случае не стоит делать. Как себя вести если Вам позвонил неизвестный и, представившись сотрудником кредитно-финансового учреждения, требует персональные данные Вашей банковской карты? Как обезопасить себя при совершении покупок либо продаж товара через Интернет?

На сегодняшний день наиболее часто встречаются следующие способы совершения дистанционных хищений:

1. Хищение совершено с использованием средств IP-телефонии и телефонов сотовых операторов под предлогом предотвращения несанкционированного списания денежных средств, оформления кредита, блокировки банковской карты, сохранения денежных средств на «резервном» счёте.

Преступник вводит жертву в заблуждение с помощью методов так называемой «социальной инженерии», получая реквизиты банковской карты и одноразовые коды в СМС, созданные для идентификации лица в системе дистанционного банковского обслуживания, как владельца, либо заставляет потерпевшего установить программы удалённого доступа «Team - Viewer» или «AnyDesk», распоряжается имеющимися на лицевом счёте денежными средствами, как правило переводя их на подконтрольные счета, используя различные платежные сервисы, электронные кошельки и номера телефонов операторов сотовой связи.

**В данном случае необходимо немедленно прекратить разговор, позвонить по номеру «горячей линии» банковского учреждения, в котором оформлена Ваша банковская карта, либо лично посетить офис банка и поинтересоваться по поводу сомнительных переводов.**

**Запомните! Сотрудники банка никогда по телефону не будут спрашивать персональные данные банковских карт, тем более код из СМС. Не существует такого вида сохранения средств, как внесение наличности через терминал на «резервный» счёт либо перевод на абонентский номер. Ни в коем случае не передавайте персональные данные своей банковской карты, не устанавливайте в своем смартфоне либо компьютере какие-либо программы по просьбе неизвестного лица.**

2. Хищение совершено посредством телефонного звонка под видом покупателя либо продавца по размещённому объявлению на торговых площадках сайтов «Авито», «Юла» и т.п.

Преступник вводит жертву в заблуждение, поясняя, что в связи с нахождением за пределами Оренбургской области, лично передать деньги не может и предлагает осуществить сделку дистанционно. Для этого, как правило, лица переходят для общения в мессенджеры, чаще «WhatsApp», договариваются о получении (отправке) товара с помощью служб доставки (Avito – доставка, CDEK, Boxberry и т.п.), преступники скидывают интернет – ссылку на фишинговые (поддельные) сайты, где жертва вносит реквизиты банковской карты.

**Запомните! Торговые площадки оснащены системой защиты от сомнительных операций по переводу средств, позволяющей блокировать различные ссылки, поэтому если Вас покупатель/продавец просит перейти к общению в мессенджере и кидает ссылку, то это первый тревожный сигнал к тому, что Вас хотят обмануть. Зачастую ссылки, отправляемые преступниками, по названию могут быть схожи с названиями различных компаний по доставкам товара, даже с названиями самих торговых площадок. Не переходите по ссылкам, отправленным неизвестными лицами.**

3. Хищение совершено посредством телефонного звонка под предлогом выдачи кредитов (займов).

В данной ситуации, до совершения преступления, потерпевший самостоятельно находит предложения в интернет среде о предоставлении кредита, перейдя на «фишинговый» сайт, оставляет свои контакты. Злоумышленник, под видом работника кредитного учреждения, связывается с жертвой, выманивает реквизиты карты под предлогом оплаты комиссии и распоряжается деньгами через подконтрольные банковские счета.

**В данном случае надо знать, что ведя переговоры по телефону по поводу доставки кредитных денежных средств и заранее оплачивая услуги курьера, сумму за страхование и открытие счёта, без документального подтверждения, Вы рискуете остаться без денег. Самый надёжный способ получения кредита – это личное посещение банка.**

4. Хищение совершено с использованием «фишинговых сайтов» в сети Интернет. Как правило это «двойники» сайтов продаж авиабилетов, сайтов интернет - магазинов бытовой техники, электрооборудования и электроинструментов. Различаться такие сайты от настоящих могут в одну букву или цифру. Домены таких сайтов обычно зарегистрированы за пределами Российской Федерации.

**Необходимо помнить и знать, что самый надёжный способ приобретения билетов – это касса аэропорта, железнодорожного транспорта. Если же Вы решили купить билет в сети Интернет, то необходимо внимательно изучить сайт, почитать отзывы.**

5. Хищение совершено с использованием сети Интернет в социальных сетях («Одноклассники», «ВКонтакте», «Инстаграм»), в том числе путём взлома страниц.

В этой ситуации прослеживается закономерность: в «Одноклассниках» жертвами становятся лица пожилого возраста, предлогом является мнимая выплата всякого рода компенсаций (НДС, доплаты к пенсии и т.п.). Во «Вконтакте» злоумышленником взламывается страница связей потерпевшего и от их имени, путём переписки, запрашиваются денежные средства в долг, с указанием реквизитов банковской карты. В социальной сети «Инстаграм» распространены так называемые интернет – страницы продаж вещей, где под видом сделки преступники завладевают реквизитами банковских карт либо вынуждают внести предоплату за товар и не исполняют своих обязательств.

**Если Ваш знакомый в социальной сети просит деньги в долг, необходимо связаться с ним по телефону, либо убедиться в ходе переписки, что с Вами общается именно он, а не мошенник, у которого в пользовании находится взломанная страница знакомого.**

6. Хищение совершено посредством телефонного звонка, под предлогом освобождения родственника от уголовной ответственности. Преступники звонят, как правило, на домашние телефоны, представляются сотрудниками правоохранительных органов, доводят ложную информацию о том, что родственник собеседника якобы попал в беду (ДТП, сбил человека, избил кого-либо и т.п.). В данном случае преступники предлагают решить вопрос, для чего требуется определенная сумма денег, которую в последующем забирают через таксистов, либо предлагают зачислить денежные средства на банковские реквизиты.

**Будьте внимательны! При поступлении подобных звонков, несмотря на уговоры преступников о том, что не стоит звонить никому, немедленно свяжитесь с родственником, который попал в «беду».**

**В разговоре сохраняйте спокойствие и не называйте данные родственника, скажите неизвестному, что будете по данному факту обращаться в правоохранительные органы.**

7. Хищение совершено под видом предоставления различных услуг, например по оформлению документов для трудоустройства.

Данные преступления совершаются в результате размещения на интернет-сайтах по предоставлению услуг объявлений по специально заниженной стоимости. В результате последующего обмана жертвы мошенников перечисляют задаток либо всю сумму, не получая результата.

**Запомните! Ни в коем случае не стоит перечислять денежные средства, не убедившись в том, что на самом деле существует организация, услугами которой Вы хотите воспользоваться. Проверьте организацию путём мониторинга сети Интернет, почитайте отзывы, попробуйте связаться с представителями и поинтересуйтесь, каким видом деятельности занимается организация и какие услуги предоставляет.**

**Сообщение для трансляции в СМИ и сети Интернет**

**На территории области участились случаи мошенничеств и краж со счетов граждан.**
**УМВД России по Оренбургской области предупреждает, будьте бдительны, не дайте себя обмануть!**

**СИТУАЦИЯ 1.**

Вам поступил звонок с неизвестного номера (495***, 499***, 8800***) от «сотрудника банка», который сообщает о незаконных операциях по Вашему счету, предлагая пройти процедуру отмены незаконной операции и возврата похищенных денежных средств. В ходе разговора неизвестный пытается выяснить реквизиты банковских карт (номер, срок действия и код с оборотной стороны), а также коды, поступающие в СМС-сообщении.

**Никогда не сообщайте никакую информацию по телефону неизвестному, даже если звонок поступил с «официального» номера кредитно-финансового учреждения. При возникновении подобной ситуации обратитесь в отделение банка лично, или позвонив по телефонному номеру, указанному в договоре обслуживания, а также на обороте платежной карты.**

**СИТУАЦИЯ 2.**

По телефону Вам предлагают выдать кредит (займ) под низкий процент и под предлогом оплаты комиссии, услуг курьера, стоимости страхования просят перечислить денежные средства на банковские карты (счета).

**Помните! Ведя переговоры по телефону по поводу доставки кредитных денежных средств и заранее оплачивая услуги курьера, сумму за страхование и открытие счёта, без документального подтверждения, Вы рискуете остаться без денег. Самый надёжный способ получения кредита – это личное посещение банка.**

**СИТУАЦИЯ 3.**

Вы решили купить в Интернет-магазине новый мобильный телефон, ноутбук, фотоаппарат, или любой другой товар по привлекательной цене, но сотрудник магазина просит перечислить предоплату.

**Никогда не перечисляйте деньги на электронные кошельки и счета мобильных телефонов. Помните, что интернет-магазин не может принимать оплату за покупку в такой форме. Если Вас просят оплатить товар с использованием терминалов экспресс-оплаты, или перевести деньги на электронный кошелек, вероятность того, что Вы столкнулись с мошенниками крайне высока.**

**СИТУАЦИЯ 4.**

Вы решили продать/купить товар через сеть Интернет на торговых площадках «Авито», «Юла» и т.п., Вам звонит покупатель/продавец, сообщая о том, что готов оплатить/купить товар, но для этого ему необходимо узнать реквизиты банковской карты для безналичного перевода/оформления доставки (номер, срок действия и код с оборотной стороны), а также коды поступающие в СМС-сообщении. Для получения оплаты/получения товара необходимо выполнить определенные действия у банкомата, либо по перейти по ссылке.

**Никогда никому не сообщайте реквизиты карты, иначе денежные средства со счета будут похищены. Для перевода денег покупателю достаточно знать только номер карты, никакие другие сведения не требуются. Если Вас просят пройти к ближайшему банкомату, терминалу оплаты, либо перейти по ссылке для оплаты (отправки товара через транспортную компанию), можете не сомневаться, Вы имеете дело с мошенником! Никогда не выполняйте указания неизвестного по телефону.**

**СИТУАЦИЯ 5.**

Общаетесь в Интернете и ведёте аккаунты в соцсетях («ВКонтакте», «Одноклассники»). К Вам обратился знакомый с просьбой одолжить ему денежные средства, либо назвать свои данные карты для осуществления перевода.

**Никогда не переводите деньги на неизвестные Вам счета, предварительно не удостоверившись в том, что денежные средства требуются именно Вашему другу, связавшись с ним по телефону, даже если в сообщении он пишет, что не может говорить. Никогда не размещайте в открытом доступе и не передавайте информацию личного характера, которая может быть использована во вред (фото паспорта и любых других документов). Общение в сети в значительной мере обезличено и за фотографией профиля может скрываться кто угодно.**

**СИТУАЦИЯ 6.**

Вам позвонили на телефон (сотовый или городской) под видом родственника и сказали, что попали в ДТП, в полицию и просят за решение вопроса перечислить денежные средства на карты, телефоны и др. счета.

**Помните, что прежде чем расстаться с деньгами, необходимо связаться с родственником под видом, которого звонят злоумышленники и убедиться что с ним все в порядке. Также можно задать контрольный вопрос якобы родственнику (дата рождения, имя матери, адрес проживания) и злоумышленник сам закончит разговор.**

**СИТУАЦИЯ 7.**

**В сети Интернет Вы нашли объявление о предоставлении услуг, с Вами связались по телефону и предлагают оплатить денежную сумму** за оформление документов для трудоустройства.

**Ни в коем случае не стоит перечислять денежные средства, не убедившись в том, что на самом деле существует организация, услугами которой Вы хотите воспользоваться. Проверьте организацию путём мониторинга сети Интернет, почитайте отзывы, попробуйте связаться с представителями и поинтересуйтесь, каким видом деятельности занимается организация и какие услуги предоставляет.**