Министерство здравоохранения Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Северный государственный медицинский университет»
Министерства здравоохранения Российской Федерации

ШКОЛА ЗДОРОВЬЯ

Университетские субботы

Архангельск
2018

ФИНАНСОВАЯ ГРАМОТНОСТЬ

Надежный фундамент Вашего Успеха!

Правила финансовой безопасности

Коновалова Людмила Владимировна

доцент кафедры экономики и управления

к.э.н., доцент

Финансовая безопасность

Наша финансовая безопасность напрямую зависит от принимаемых нами ежедневно решений.

Неприятная финансовая ситуация может возникнуть в результате

финансового мошенничества

Финансовое мошенничество

Финансовое мошенничество — совершение противоправных действий в сфере денежного обращения путем обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения.

Наиболее частыми являются следующие виды:

1. Мошенничества с использованием банковских карт

2. Интернет-мошенничества

3. Мобильные мошенничества

1. Мошенничества с использованием банковских карт

Банковская карта – удобный инструмент повседневных расчетов.

Наиболее распространены:

- **Дебетовые** - инструмент управления банковским счетом, на котором размещены собственные средства держателя карты.
- **Кредитные** - позволяют на основании заключенного с банком договора брать в долг у банка определенные суммы денег в пределах установленного кредитного лимита.

1. Мошенничества с использованием банковских карт

Способы обмана людей и кражи денег с их банковских карт разнообразны: от подглядывания из-за плеча во время операций с банкоматом и последующего хищения карты до хакерских атак на программное обеспечение.

При этом преступники постоянно придумывают новые способы хищения денежных средств, по мере того как старые перестают работать.

Основные виды:

- **Скимминг**
- **Ливанская петля**
- **«Магазинные» мошенники**
- **Фишинг**
- **Мошенничество с помощью телефона**
- **Вишинг**

1. Мошенничества с использованием банковских карт

скимминг

Скимминг – это мошенничество с использованием специального устройства «скиммера», которое позволяет считывать данные с магнитных лент банковских карт и ПИН-коды прямо в банкомате и затем снимать с этих карт деньги.

Предполагает установку специальных устройств на банкоматы, с помощью которых преступники получают информацию о карте.

Это может быть накладная клавиатура (очень похожая на настоящую) и устройство для считывания данных карты, которое устанавливается на картридер.

Вместо клавиатуры может быть установлена миниатюрная камера, которая заснимет процесс ввода ПИН-кода.

При использовании банкомата осмотрите поверхность над ПИН-клавиатурой и устройство для приема карты на предмет нахождения посторонних предметов.

1. Мошенничества с использованием банковских карт

ТРАППИНГ (ЛИВАНСКАЯ ПЕТЛЯ)

Отрезок фотопленки (складывается пополам, края загибаются под углом в 90 градусов) вставляется в банкомат. На нижней стороне фотопленки вырезан небольшой лепесток, отогнутый вверх по ходу карты. Пленка располагается в картридере так, чтобы не мешать проведению транзакции. Отогнувшийся лепесток не позволяет банкомату выдать пластиковую карту обратно.

или помощь прохожего

Суть этого вида мошенничества заключается в установке на банкомат устройства, которое блокирует карту и не выдает ее обратно.

На помощь человеку приходит «добрый» мошенник, раздавая различные советы.

В процессе «помощи» растерянный человек обычно соглашается на введение ПИН-кода, который и запоминает преступник.

После чего мошенник «уходит», советуя обратиться в банк.

Растерянный человек оставляет карту в банкомате, а мошенник спокойно ее достает и использует по своему усмотрению.

Закрывайте рукой клавиатуру при вводе ПИН-кода!!!

1. Мошенничества с использованием банковских карт

МАГАЗИННЫЕ МОШЕННИЧЕСТВА

От недобросовестных сотрудников в организациях не застрахован никто.

Данные карты могут быть считаны и зафиксированы ручным скиммером, а впоследствии использованы для хищения денег.

- **Не передавайте карту посторонним: ее реквизиты (номер карты, срок действия, имя владельца и т.д.) могут быть использованы для чужих покупок.**
- **Требуйте проведения операций с картой только в личном присутствии, не позволяя уносить карту из поля зрения (например, официантам или кассирам).**

1. Мошенничества с использованием банковских карт

Фишинг

Самая сложная задача мошенника — узнать ваш ПИН-код.

Никому не сообщайте свой ПИН-код!!!

ФИШИНГ

Цель фишинга — получить данные о пластиковой карте от самого пользователя.

В этом случае злоумышленники рассылают пользователям электронные письма, в которых от имени банка сообщают об изменениях, якобы производимых в системе его безопасности.

При этом мошенники просят доверчивых пользователей возобновить информацию о карте, в том числе указать номер кредитки и ее ПИН-код.

Сделать это предлагается несколькими способами: либо отправив ответное письмо, либо пройдя на сайт банка и заполнив соответствующую анкету.

Однако ссылка, прикрепленная к письму, ведет не на ресурс банка, а на поддельный сайт, имитирующий работу настоящего.

1. Мошенничества с использованием банковских карт

МОШЕННИЧЕСТВО С ПОМОЩЬЮ ТЕЛЕФОНА

Разновидностью фишинга являются звонки на сотовые телефоны граждан от «представителей» банка с просьбой погасить задолженность по кредиту.

Когда гражданин сообщает, что кредит он не брал, ему предлагается уточнить данные его пластиковой карты.

В дальнейшем указанная информация используется для получения несанкционированных денежных переводов с карточного счета пользователя.

Банки и платежные системы никогда не присылают писем и не звонят на телефоны своих клиентов с просьбой предоставить им данные счетов.

Если такая ситуация произойдет, вас *ПОПРОСЯТ* приехать в банк *лично*.

1. Мошенничества с использованием банковских карт

ВИШИНГ (ГОЛОСОВОЙ ФИШИНГ)

Новый вид мошенничества, использующий технологию, позволяющую автоматически собирать информацию, такую, как номера карт и счетов.

Мошенники моделируют звонок автоинформатора, получив который держатель получает следующую информацию:

Автоответчик предупреждает потребителя, что с его картой производятся мошеннические действия, и дает инструкции — перезвонить по определенному номеру.

Злоумышленник, принимающий звонки по указанному автоответчиком номеру, представляется вымышленным именем от лица финансовой организации.

Когда по этому номеру перезванивают, на другом конце провода отвечает типичный компьютерный голос, сообщающий, что человек должен пройти сверку данных и ввести 16-значный номер карты с клавиатуры телефона.

Затем, используя этот звонок, можно собрать и дополнительную информацию, такую, как срок действия карты, дата рождения, номер банковского счета и т. п.

1. Мошенничества с использованием банковских карт

Структура мошенничества с банковскими картами в России

Всего - 4,48 млрд. руб.

- **38%** - фальшивые карты
- **47%** - потерянные или украденные карты
- **15%** - кредитные карты, полученные по поддельным документам

1. Мошенничества с использованием банковских карт

МЕРЫ БЕЗОПАСНОСТИ

- Храните ПИН-код отдельно от карты и не пишите его на карте, не сообщайте никому и не вводите ПИН-код при работе в Интернете. При его потере или краже – заблокируйте карту
- Сохраняйте все документы до окончания проверки правильности списанных сумм
- Сообщайте банку актуальные контактные данные
- Подключите услугу SMS- уведомлений, всегда имейте при себе телефон службы поддержки
- В случае мошеннической или ошибочной операции по карте уведомите банк до конца следующего дня, чтобы сумма этой операции была полностью возмещена банком, иначе вернуть деньги будет гораздо сложнее.

2. Интернет-мошенничества

Мошенничество в интернете включает в себя все существующие виды обмана, придуманные человечеством за всю историю его существования. Этот перечень обширен, поскольку мошенники по максимуму используют все преимущества интернет-коммуникаций: массовый охват, возможность выбора целевой группы, оперативность.

ОСНОВНЫЕ ВИДЫ ИНТЕРНЕТ-МОШЕННИЧЕСТВ:

- **Покупки через интернет**
- **Составляем гороскоп**
- **Письма от платежных систем, судебных приставов и др.**
- **«Нигерийские» сюжеты**

2. Интернет-мошенничества

ПОКУПКИ ЧЕРЕЗ ИНТЕРНЕТ

Покупатель (жертва) соглашается купить у продавца (мошенника) товар через интернет.

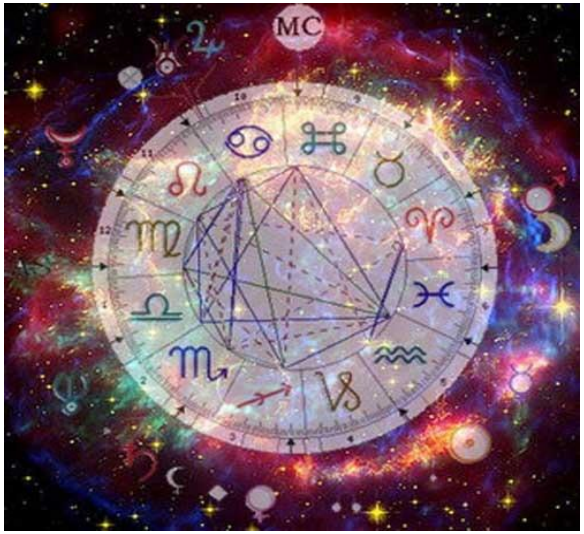
Продавец просит оплатить товар через систему денежных переводов и получает деньги, используя зачастую фальшивое или недействительное удостоверение личности.

Обещанный товар не доставляется покупателю.

Такая схема мошенничества обычно имеет один или несколько явных признаков — например, предлагаемый товар продается по **удивительно низкой цене.**

2. Интернет-мошенничества

СОСТАВЛЕНИЕ ГОРОСКОПА



Объявлений, предлагающих заказать персональный гороскоп, очень много во всемирной паутине.

Авторы обещают выслать его быстро и бесплатно. Пользователю предлагается заполнить стандартную анкету (имя, фамилия, дата рождения), оставить свой электронный адрес.

Любитель астрологии указывает все эти данные, но вместо гороскопа в его ящик попадает письмо с еще одним условием: чтобы получить заказ, надо отправить по указанному номеру СМС-сообщение с набором тех или иных цифр.

При этом забывают добавить, что ***стоимость*** этого сообщения может составлять **несколько сотен рублей.**

В лучшем случае ему, действительно, пришлют гороскоп. Причем сразу же, что уже вызывает сомнения в его уникальности. В худшем — ничего не пришлют.

2. Интернет-мошенничества

ПИСЬМА ПЛАТЕЖНЫХ СИСТЕМ

Вы можете обнаружить в своем почтовом ящике письмо от администрации платежной системы (e-gold, Moneybookers, Paypal), судебных приставов и других...

В послании, например, говорится, что у вас есть долг по кредиту и вам нужно срочно сверить данные в файле.

К письму прилагается вложение — файл, который нужно скачать и открыть. Или же в письме есть ссылка, по которой нужно перейти «для скачивания программы».

На самом деле часто вас поджидает **вирус,** задача которого - собрать данные о ваших аккаунтах в платежных системах, **данные банковской карты,** которые вы вводите на своем компьютере.

Аккаунт *– это личный кабинет на каком-либо web-портале, который позволяет совершать действия, недоступные для незарегистрированных пользователей (хранить файлы в нем и скачивать на свой ПК), а также пользоваться специализированными сервисами*

2. Интернет-мошенничества

«НИГЕРИЙСКИЕ» СЮЖЕТЫ

Суть этой мошеннической схемы сводится к тому, что некто представляется получателю письма действующим или бывшим министром или представителем знатной нигерийской (зимбабвийской, кенийской...) семьи, попавшей в немилость на родине.

К адресату обращаются с просьбой оказать содействие в выводе из охваченной гражданской войной страны крупной суммы, которая будет переведена на счет адресата.

Ему за помощь «в спасении средств» обещают солидный процент.

Когда клиент «заглатывает наживку», его просят перечислить незначительную сумму, необходимую для оформления перевода, дачи взятки или оплаты услуг юриста.

Затем появляется еще одна причина перечислить «незначительную» сумму, потом другая... Деньги тянут из доверчивого клиента до тех пор, пока он не осознает, что его обманули.

По результатам специальных исследований, примерно один процент пользователей интернета, то есть **каждый сотый**, получивших по e-mail «нигерийские письма», оказываются вовлеченными в эту аферу.

В арсенале мошенников как правило несколько уловок, которые могут сочетаться в одном письме.

2. Интернет-мошенничества

СПОСОБЫ ЗАЩИТЫ

- Старайтесь **не открывать сайты платежных систем по ссылке** (например, в письмах). Обязательно проверяйте, какой URL стоит в адресной строке (URL – это адрес какого-либо ресурса в интернете), или посмотрите в свойствах ссылки, куда она ведет. Вы можете попасть на сайт-обманку, внешне очень похожий, практически неотличимый от настоящего сайта платежной системы. Расчет в этом случае на то, что вы введете на таком сайте свои данные и они станут известны мошенникам.

- **Совершайте покупки в интернете с помощью отдельной банковской карты и только на проверенных сайтах**

- **Никогда никому не сообщайте ваши пароли.** Вводить пароли можно и нужно только на самих сайтах платежных процессоров, но никак не на других ресурсах.

- **Не храните файлы с секретной информацией на доступных или недостаточно надежных носителях информации.** Всегда делайте несколько копий таких файлов на разных носителях.

2. Интернет-мошенничества

СПОСОБЫ ЗАЩИТЫ

- Если вам предлагают удаленную работу и при этом просят оплатить регистрационный взнос в качестве гарантии за пересылку данных и т. п., не попадайтесь на эту ловушку.

  Настоящие работодатели никогда не просят денег с соискателей, они сами платят за работу!

- Предложения в духе «вышлите туда-то небольшую сумму и вскоре вы будете завалены деньгами» — это предложения от участников финансовых пирамид. Не верьте таким предложениям, **в пирамидах выигрывают только их создатели.**

- Письма о проблемах с вашим счетом в какой-либо платежной системе, требующие перехода на сайт и каких-либо действий от вас, отправляйте в корзину, не открывая.

  Техническая поддержка платежных систем никогда не рассылает таких писем.

- В 99 % случаев платежи, которые вы делаете онлайн, отменить нельзя. Поэтому не торопитесь, **подумайте, прежде чем заплатить за товар или услугу.**

3. Мобильные мошенничества

По данным международной статистики, совокупные потери операторов связи и абонентов от мобильного мошенничества ежегодно составляют **примерно 25 млрд. долларов.**

ОСНОВНЫЕ ВИДЫ МОБИЛЬНЫХ МОШЕННИЧЕСТВ:

- **«Вы выиграли приз...»**
- **«Мама, я попал в аварию...»**
- **«Ваша банковская карта заблокирована...»**
- **Вирус**

3. Мобильные мошенничества

«ВЫ ВЫИГРАЛИ ПРИЗ...»

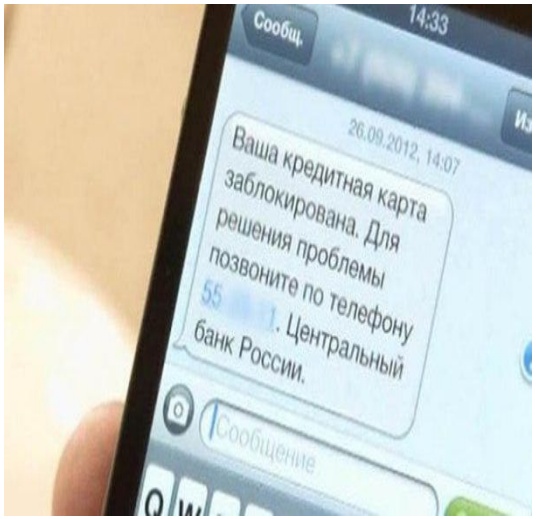
Мошенник привлекает «жертву» дорогим подарком, который выиграл абонент, но при этом просит прислать подтверждающую СМС, внести «регистрационный взнос» через интернет-кошелек, купить карточку предоплаты и перезвонить, назвав код.

Получив «взнос», мошенник исчезает, а обещанный приз тоже растворяется.

«МАМА, Я ПОПАЛ В АВАРИЮ...»

Эта схема направлена на воздействие на психику человека. Мошенник отправляет СМС или звонит с неприятной новостью, «жертва» в панике забывает проверить достоверность полученной информации и переводит средства на счета мошенников.

3. Мобильные мошенничества



«ВАША КАРТА ЗАБЛОКИРОВАНА»

На мобильный телефон приходит СМС «Ваша банковская карта заблокирована. По вопросам разблокировки обращайтесь по телефону...». «Жертва» перезванивает по указанному номеру и «сотрудник банка», которым является мошенник, предлагает пройти к банкомату и совершить несколько операций под диктовку. Результат не заставит себя долго ждать - деньги с карты перейдут на счет мошенников.

ВИРУС

Он помогает злоумышленникам подобраться к банковской карте, привязанной к мобильному телефону, и перевести все деньги на свой счет.

Правила финансовой безопасности

- Проявляйте бдительность и внимательность к своим ежедневным финансовым операциям.
- Никогда никому не сообщайте ваши пароли, ПИН-код и другую информацию о вашей карте.
- Используйте антивирусное программное обеспечение.
- При совершении платежей в интернете обязательно проверяйте, какой URL (URL – это адрес какого-либо ресурса в интернете) стоит в адресной строке.
- Не передавайте банковскую карту третьим лицам.
- Обязательно установите пароль для разблокировки телефона, особенно если на нем установлено банковское мобильное приложение.
- При получении сомнительных СМС от банков или лиц, представившихся родственниками, позвоните в банк или родственникам, уточните информацию. Не отвечайте на сомнительные СМС.
- Если Вы стали жертвой финансовых мошенников, сообщите в полицию.

Спасибо за внимание!