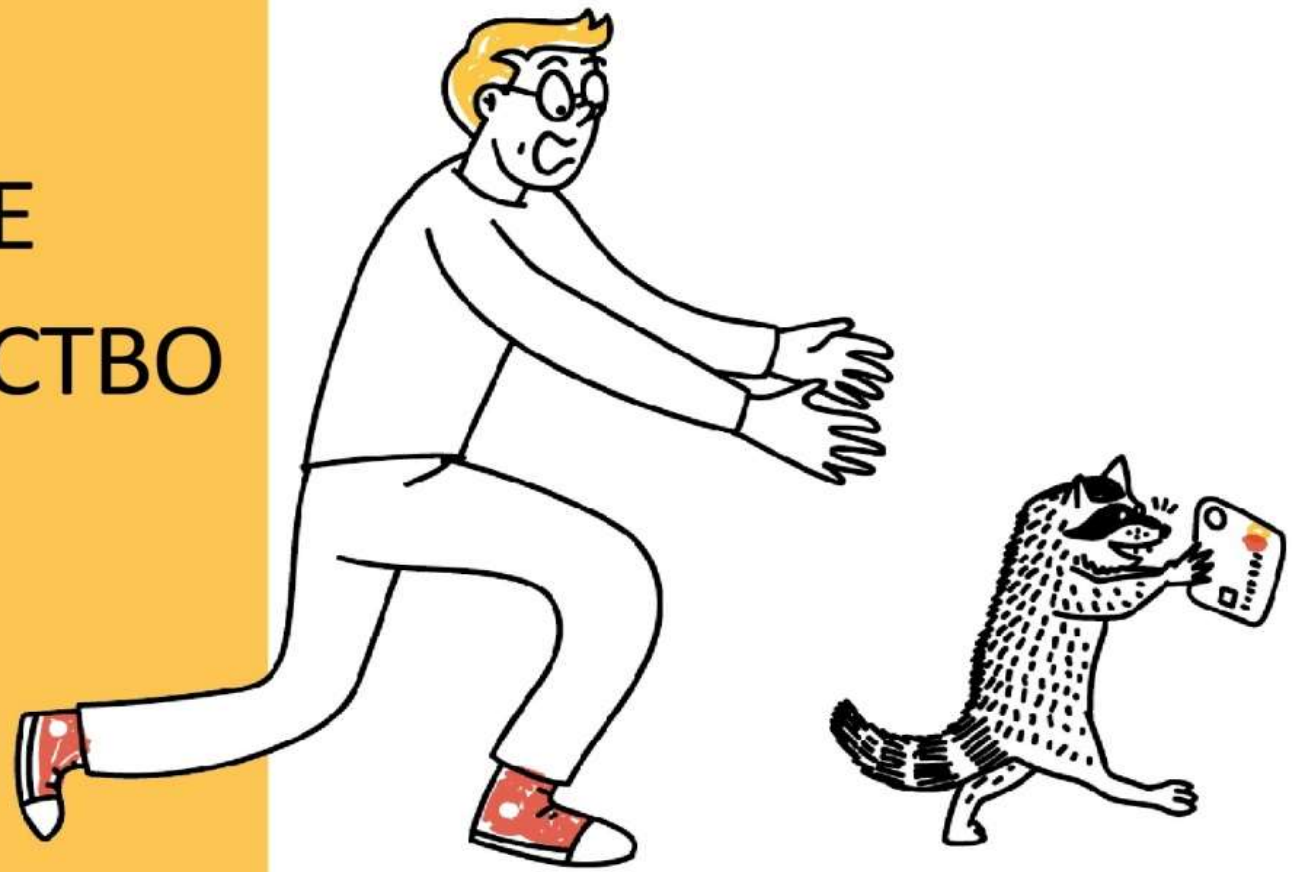
Банк России

ФИНАНСОВОЕ МОШЕННИЧЕСТВО

Защитите себя
и свою семью



Тема урока «Современные виды финансового мошенничества»

- Имущества, обмана, чужого, доверием, злоупотребление, хищение, или, путем

Задание: сложить из данных слов определение слова *«мошенничество»*

Мошенничество – это хищение чужого имущества путем обмана или злоупотребления доверием

Задание: определить, мошенник или нет?

Вы гуляли по парку и увидели плакаты «Собираем деньги на приют для животных». Рядом - несколько человек, которые агитируют за сбор средств для приюта для животных.

- - Здравствуйте! Вы любите животных? А знаете ли вы, сколько животных в год оказывается на улице? Добрые хозяева просто выбрасывают на улицу неугодных зверей, а мы подбираем их и пристраиваем. А на все огромные деньги нужны! Мы создали благотворительную организацию, чтобы помощь была оказана как можно большему количеству животных. И именно вы можете нам помочь! Принимаем только наличные средства! Приют находится за городом, где чистый воздух. Директор наш – отличный человек, недавно подобрал 7-х котят!Помогите песикам и котикам!

Задание:определить, мошенник или нет?

Выходной день. Вы прогуливались по торгово-развлекательному центру и увидели, что проводится какое-то мероприятие. Решили подойти поближе и поучаствовать.

- - Добрый день, друзья! Сегодня исполняется 15 лет нашему любимому магазину «Продукты для всей семьи». В честь этого знаменательного события сегодня проводятся конкурсы с приятными сюрпризами и лотерея с настоящими подарками! Для того чтобы принять участие в лотереи, вам нужно купить в магазине товарына сумму 2500 рублей. Прийти ко мне, заполнить короткую анкету, прикрепить к ней чек и бросить в наш барабан – лототрон. Каждые 3 часа мы проводим розыгрыш. Следующий в 15.00.

Прием «ФИШБОУН»

Прием «ФИШБОУН»

Задание для групп: познакомьтесь с ситуацией, связанной с мошенничеством и определите факт, причину мошенничества и сделайте вывод, как можно обезопасить себя. Ответы запишите на полоске соответствующего цвета

- **Красная полоса - Факт(в чем состоит мошенничество)**
- **Желтая полоса - Причина (Почему это произошло)**
- **Зеленая полоса - Вывод(Как себя обезопасить)**

Ситуация 1

- Наташа загорелась идеей купить беговую дорожку. Девушка нашла на «Авито» вариант, который ей понравился. Товар находился в другом городе. Девушка-продавец предложила доставку и перейти для общения из «Авито» в WhatsApp. В итоге они договорились, что закажут доставку, Наташе прислали ссылку на сайте, внешне очень похожем на сервис Boxberry. Сервис потребовал оплатить доставку и товар. Причем там было указано, что деньги за товар перейдут продавцу только после проверки со стороны покупателя. Наташа нажала "оплатить", ввела данные карты и ее перебросило на страницу, банк прислал код (как это обычно происходит при оплате товаров через интернет), но письмо с подтверждением не пришло. Девушка позвонила продавцу, она уже не брала трубку, не отвечала в мессенджере и удалилась с «Авито». Итог – потерянные 12 тысяч рублей и никакой беговой дорожки.

Ситуация 2.

- Маша все свободное время проводит в социальных сетях, таких как " Одноклассники"," ВКонтакте", "Инстаграмм" и т.д.Здесь она с удовольствием рассказывает о себе, делится своими фотографиями, контактными данными (телефоном, почтой) с целью поиска новых друзей и знакомых. Маша любит также делиться своими планами, рассказывает о том, куда собирается пойти и где с ней можно встретиться. Однажды Машиной маме позвонили на домашний телефон незнакомые, которые представились сотрудниками полиции, и рассказали ей о том, что с Машей стряслась беда, ее обвиняют в краже косметики в одном из супермаркетов. Неизвестные предложили маме выход из ситуации - перевести определенную сумму денег на банковский счет. При этом незнакомцы приводили факты из личной жизни Маши, поэтому мама не усомнилась в правдивости их слов и перевела деньги. Только потом она позвонила Маше, и обман раскрылся.

Ситуация 3

- В полицию обратилась женщина 1963 года рождения, жительница г. Томска. Она рассказала, что неизвестные позвонили ей на сотовый телефон и, представившись сотрудниками банка, попросили о помощи в разоблачении неких жуликов. Голос по телефону убедил томичку, что на ее счетах были замечены подозрительные операции. Действуя по указке "сотрудника банка", женщина сняла все свои сбережения с одного счета и посредством банкомата перевела их на другой, якобы безопасный, счет. Таким образом она потеряла 6,5 миллиона рублей.

Ситуация 4

- 46-летняя Валентина решила продать в интернете лодочный мотор. Некоторое время спустя после публикации объявления женщина получила смс - сообщение со ссылкой, по которой она перешла. Сразу же пришло другое сообщение о том, что с ее счета списаны деньги (8 тысяч рублей). Оказалось, что после перехода по незнакомой ссылке телефон потерпевшей оказался заражен вирусом, с помощью которого злоумышленники и получили доступ к мобильному банку женщины.

Ситуация 5

- В интернете Петр искал подработку, пока не наткнулся на один сайт, где после заполнения анкеты соискателя появилось сообщение о призе в 32 тысячи рублей. Чтобы получить деньги, надо было всего-то ввести реквизиты банковской карты. Без задней мысли Петр все данные ввел, после чего на его телефон пришел одноразовый код, который мужчина ввел на сайте. С его счета тут же исчезли 16,5 тысячи рублей.
- Мужчина два дня ждал призовых денег, пока не решил почитать отзывы о том сайте, где ему обещали приз. Тогда он и понял, что стал жертвой мошенников. Но поиски дополнительного заработка не прекратил. Уже на другом ресурсе ему пообещали 30 тысяч рублей в обмен на 3 тысячи. Недолго думая, Петр попытался перевести эти деньги с другой карты, но операцию заблокировал банк: из финансовой организации пришло сообщение, что адресат подозревается в мошенничестве.

Ситуация 6

- Максиму пришло СМС, что на его счёт поступил платёж на 500 рублей. Через некоторое время раздался звонок, что деньги ему положили нечаянно, перепутав номер, и теперь просят вернуть их мобильным переводом. Максим, как человек честный, выполнил просьбу, деньги вернул и только тогда узнал, что деньги на его счёт не поступали, просто пришло СМС о пополнении.
  А кто это СМС отправил, неизвестно.

Ситуация 7

- Галине приходит SMS с просьбой перезвонить на указанный номер мобильного телефона. Просьба была обоснована тем, что изменились тарифы связи и теперь необходимо уточнить данные. Галина добросовестно перезвонила на указанный номер, но ее долго держали на линии связи без ответа. Когда ей надоело ждать, она отключилась - и оказалось, что с ее счёта списаны крупные суммы, так как к номеру телефона был подключен мобильный банк.

Прием «ФИШБОУН»

Финансовое мошенничество – угроза нашей финансовой безопасности!

- ***Стремление сэкономить***
- *Излишняя доверчивость*
- *Знание мошенниками психологии*
- *Страх потерять деньги*
- *Невнимательность*
- *Желание получить дополнительный доход*
- *Развитие современных технологий и средств связи*

- *Поддельный платежный сайт*
- *Обман с помощью соц.сетей*
- *Звонок «сотрудника банка»*
- *Переход по незнакомой ссылке с вирусом*
- *«лотерейный» выигрыш*
- *«ошибочный « перевод средств*
- *Номер – «грабитель»*

- Позвоните в банк
- Внимательно изучать сайты Интернет-магазинов
- Никому не сообщать данные банк.карт
- Не поддаваться панике
- Помнить-бесплатный сыр в мышеловке!
- Будьте внимательны!

Разминка

Какой номер у парковочного места, в котором припаркован автомобиль? Дать ответ нужно в течение 20 секунд. (Тест на поступление в первый класс в Китае)

НАИБОЛЕЕ РАСПРОСТРАНЁННЫЕ СХЕМЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

SMS-просьба о помощи

Требование перевести определённую сумму на указанный номер, используется обращение «мама», друг», «сынок» и т.п..

Обман по телефону

Требование выкупа или взятки за освобождение из отделения полиции знакомого или родственника.

Телефонный номер-«грабитель»

Платный номер, за один звонок на который со счёта списывается денежная сумма.

Выигрыш в лотерее, которую, якобы, проводит радиостанция или оператор связи

Вас просят приобрести карты экспресс-оплаты и сообщить коды, либо перевести крупную сумму на свой счёт, а потом ввести специальный код.

Простой код от оператора связи

Предложение услуги – достаточно ввести код, который на самом деле заблокирует Вашу sim-карту

Штрафные санкции и угроза отключения номера

Якобы, за нарушение договора с оператором Вашей мобильной связи

ПОМНИТЕ! Чтобы не стать жертвой телефонных мошенников

- отметьте в телефонной книжке мобильного телефона номера всех родственников, друзей и знакомых;
- не реагируйте на SMS без подписи с незнакомого номера;
- осторожно относитесь к звонкам с незнакомых номеров.

Если Вы сомневаетесь, что звонивший - действительно ваш друг или родственник, постарайтесь перезвонить на его мобильный телефон. Если телефон отключен, постарайтесь связаться с его коллегами, друзьями или близкими для уточнения информации.

Будьте бдительны и внимательны!

Ошибочный перевод средств

Просят вернуть деньги, а потом дополнительно снимают сумму по чеку.

Услуга, якобы, позволяющая получить доступ к SMS и звонкам другого человека.

ФИШИНГ — ЭТО ВИД ИНТЕРНЕТ-МОШЕННИЧЕСТВА ЧЕРЕЗ СОЦИАЛЬНЫЕ СЕТИ И ПЛАТЕЖНЫЕ СЕРВИСЫ

КАК РАБОТАЮТ ФИШЕРЫ:

- Делают дизайн сайтов, похожий на настоящий
- Делают ссылки с неправильным написанием (Feacbook=Facebook)
- Рассылают спам в соцсетях и месенджерах
- Присылают сообщения в онлайн-играх

КАК НЕ ПОПАСТЬ НА КРЮЧОК?

- Внимательно проверяйте внешний облик сайта
- Установите Kaspersky Internet Security, чтобы сохранить свои деньги в безопасности
- Пользуйтесь только защищенными сайтами: https (где «s» означает secure — безопасное)
- Если вам пришло подозрительное письмо из банка
- Не пользуйтесь платежными сервисами и интернет-банком через публичные wi-fi сети
- Проверяйте ссылки и письма от ваших друзей и официальных организаций: банков, налоговых, он-лайн магазинов

- обратитесь в службу поддержки
- сообщите администратору страницы банка в соц. сетях

Хищения средств в интернете проходят по нескольким сценариям:

Онлайн банкинг

С помощью сайтов-зеркал (копий настоящих сайтов банков) или вредоносного ПО мошенники получают доступ к личному кабинету клиента.
Также мошенники совершают звонки, представляясь сотрудниками банка и запрашивая у клиента его идентификационные данные.

Мобильный банкинг

На мобильное устройство пользователя загружается вредоносное ПО, с помощью которого мошенники могут посредством SMS списывать деньги с банковского счета без ведома его законного владельца.

Онлайн шоппинг

При совершении покупок в онлайн-магазинах злоумышленники получают данные карты, в том числе и CVV/ CVC-код.
Другой вид обмана реализуется, когда хотят что-то купить у пострадавшего: мошенник переводит на его счет бОльшую сумму, а затем требует вернуть ему разницу. После возвращения переплаченной суммы, мошенник отзывает свой первоначальный платеж.

Открытый микрофон

- Продолжите фразу:
- Я узнал (а)…
- Я понял (а)…
- Я хочу узнать …
- Мне кажется ….

Список источников:

- УМК «Финансовая грамотность», созданные в рамках Проекта Минфина России
- Сборник методических материалов Банка России «Финансовое мошенничество. Как себя защитить», Москва, 2019
- Образовательные проекты ПАКК https://edu.pacc.ru/
- Центр «Федеральный методический центр по финансовой грамотности системы общего и среднего профессионального образования»

https://fmc.hse.ru/methodology

- РАНХиГС http://fingram.websoft.ru/