Волжский филиал ГАПОУ
«Волгоградский медицинский колледж»

16+

Как защититься от кибермошеничества. Правила безопасности в киберпространстве.

урок-предупреждение

Составитель: библиограф - Урядова Н. Г.

2022 г.

Во время летних каникул и отпусков в Интернете активизируются мошенники!

Для того чтобы не стать жертвами кибермошенников, хотим обратить ваше внимание на презентацию "Как защититься от кибермошеничества. Правила безопасности в киберпространстве".
С развитием технологий все больше финансовых услуг можно получить в электронном виде, через Интернет и мобильные приложения. Человек все больше удаленно управляет своими счетами и картами. При этом зачастую забываем о безопасности и правилах поведения в виртуальном пространстве, чем и пользуются мошенники: в 90% случаев хищение денежных средств происходит именно в виртуальной среде.
Кроме того, в результате пандемии COVID-19 ускоренными темпами развивались не только медицинские технологии, но и киберпреступники также освоили новые методы заработка.
Мы хотим обратить ваше внимание на особенно популярные категории кибермошенничества, появившихся и быстро распространившихся за два года пандемии.

Кибермошенничество.

ЭВОЛЮЦИЯ МОЩЕННИЧЕСТВА

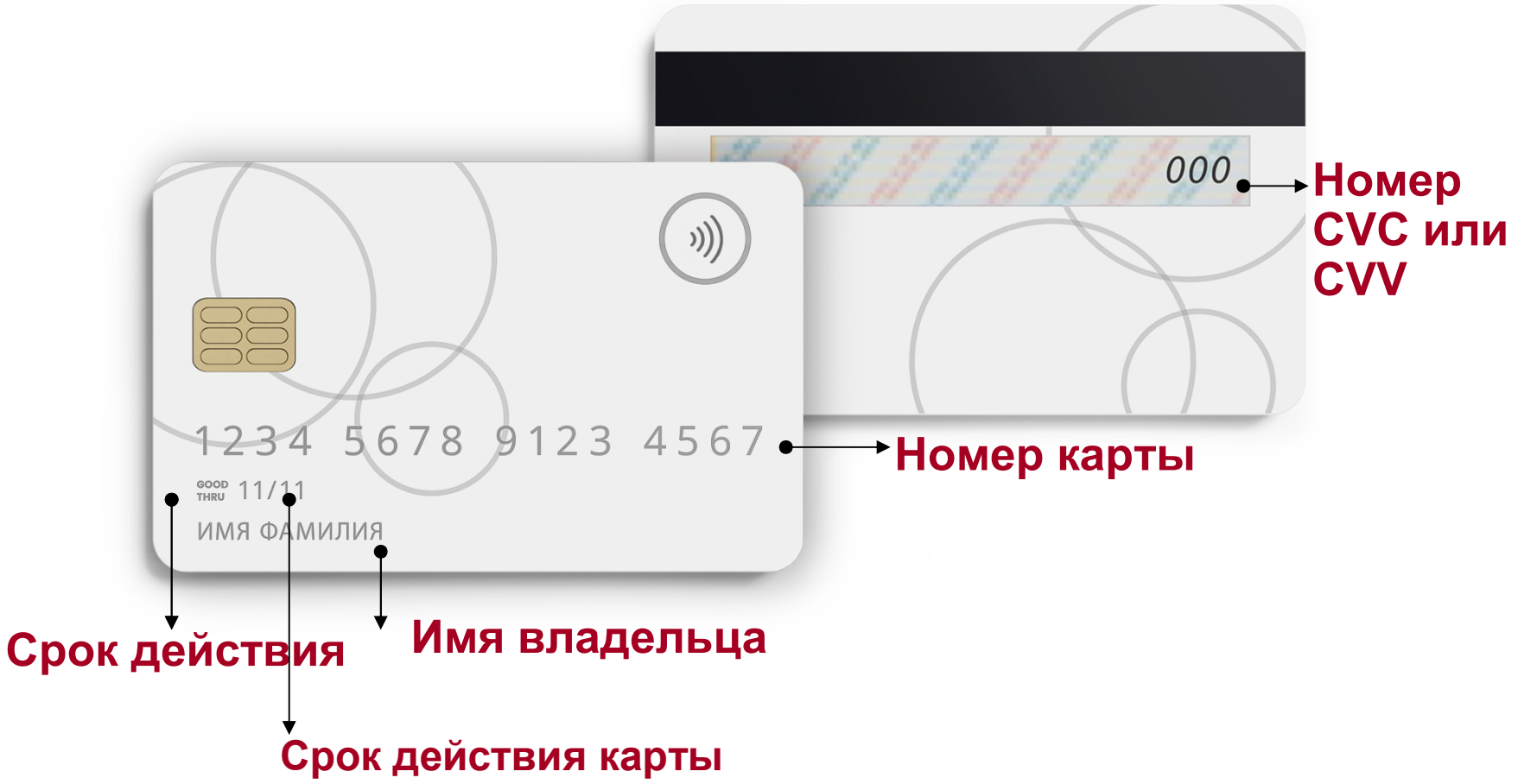
В основе мошенничества лежит обман, который был известен еще законодателям Древнего Рима.

Мошенничество **– хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.**

Финансовое кибермошенничество **– это преступная деятельность, целью которой является причинение материального или иного ущерба путем хищения личной информации пользователя.**

Совершают эти преступления киберпреступниками или ХАКЕРАМИ, которые зарабатывают на этом деньги.

БАНКОВСКАЯ КАРТА.



Обман владельца банковской карты по телефону/SMS.

Никогда не пишите PIN-код карты на самой карте
Карту можно где-то забыть или потерять. Или, к примеру, при оплате в магазине карта попадает в руки продавцов. Написанный на карте PIN-код является большим соблазном для того, чтобы без труда воспользоваться ею.

Выход простой — никогда не указывайте на карте PIN-код.

Информация из чеков.

Не выбрасывайте в урну чек, который печатает банкомат.

При оформлении новой карты и её активации прямо в банке люди обычно выбрасывают в ведро чек, выданный банкоматом. Мошенники могут подобрать выброшенную бумагу, где указана информация с логинами и паролями для входа в онлайн-банк, и перевести деньги на свой счёт.

Мошенничество при оплате безналичных счетов в гостиницах, кафе и ресторанах.

Никогда не давайте людям «подержать» свою карту

Информации, которая указана на карте, достаточно для того, чтобы совершить с её помощью покупку в интернете. **Поэтому карту лучше вообще никому не давать в руки!**

Даже в кафе опасно расплачиваться картами, когда, к примеру, официант её уносит, чтобы провести платёж. В идеале — не давать официанту карту, а самому вставлять её в устройство и вводить пароль. И обязательно — использовать карту, которая связана с вашим номером телефона.

Если кто-то другой захочет что-то оплатить вашей картой, вам придёт код-подтверждение. Игнорируйте этот код и не сообщайте его другим людям.

Мошенничество с картами в сети Интернет.

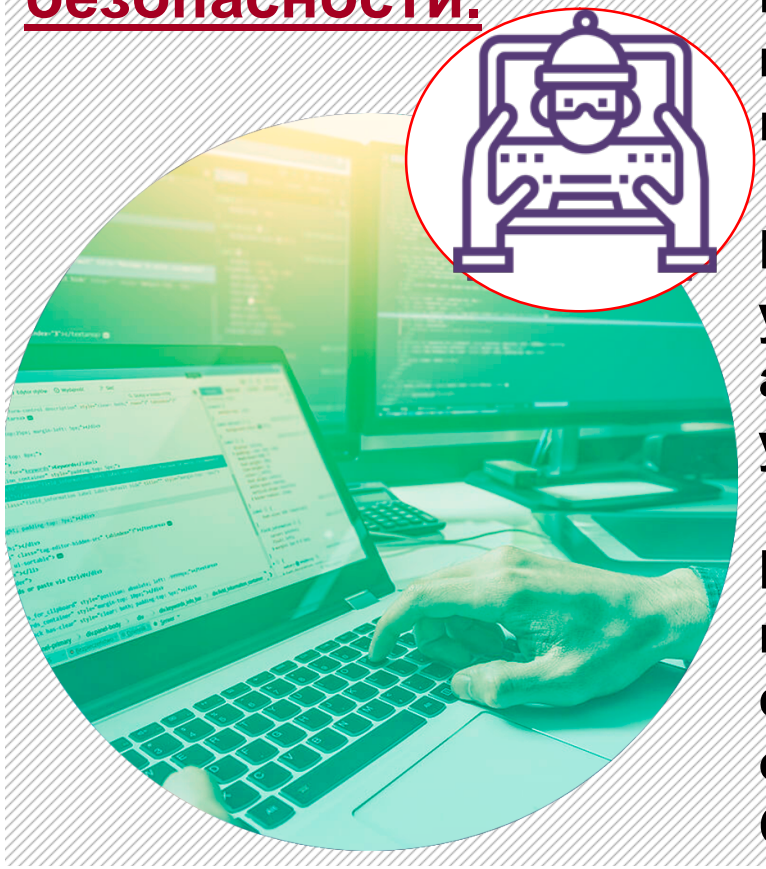
Не сообщайте данные карты и не передавайте SMS-коды неизвестным людям.
Человек размещает объявление о продаже чего-нибудь (диван, телевизор — всё, что угодно) в интернете. Мошенники звонят по указанному номеру и прикидываются покупателями. В разговоре они узнают данные карт, якобы для того, чтобы перечислить деньги за покупку.

И как только они получают эту информацию, подключаются к мобильному приложению и списывают со счёта деньги.

Никому не говорите номер карты или счёта и, что важнее, трехзначный код, расположенный на оборотной стороне карты, а также никогда никому не передавайте SMS-код, который приходит к вам от номера 900.

КАК УБЕРЕЧЬ СЕБЯ И БЛИЗКИХ ОТ ФИНАНСОВОГО МОШЕННИЧЕСТВА.

Мошенничество с банковскими картами. Правила финансовой безопасности.



Перед снятием денег в банкомате осмотрите его. На картоприёмнике не должно быть посторонних предметов, клавиатура не должна шататься.

Набирая ПИН-код, прикрывайте клавиатуру рукой. Делайте это даже во время расчётов картой в кафе.

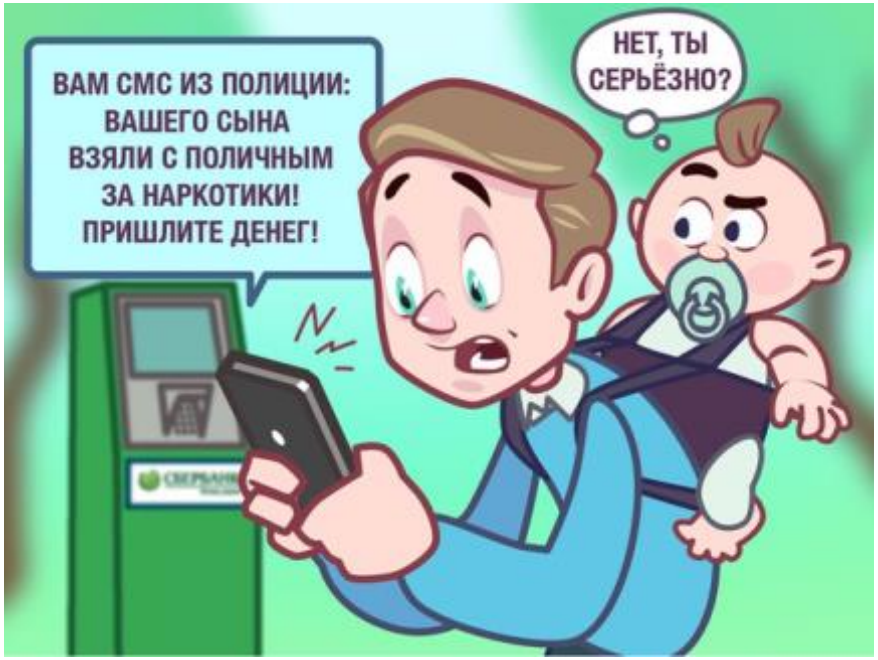
Подключите Мобильный банк и СМС-уведомления; обязательно установите антивирусную программу на мобильное устройство.

Если совершаете покупки через интернет, никому не сообщайте секретный код для подтверждения операций, который приходит вам по СМС.

Телефонные мошенничества.

Социальная инженерия: не переводите деньги незнакомым людям.

Использование социальной инженерии — один из самых распространённых способов мошенничества. Обычно человеку звонит мошенник, представляется полицейским или, к примеру, следователем и говорит, что ваш родственник или друг устроил аварию, кого-то избил или как-то ещё нарушил закон. Чтобы уладить вопрос «по-хорошему», мошенники просят перечислить с карты определённую сумму денег.



Будьте бдительны: если попадёте на такой звонок, обязательно свяжитесь для начала с человеком, которого пытаетесь спасти. Вероятно, с ним всё в порядке, а вас просто кто-то пытается обмануть.

Обман владельца банковской карты по телефону/SMS.

Не доверяйте сомнительным сообщениям о блокировке карты.

Мошенники могут присылать SMS-сообщения о том, что банковская карта заблокирована. На самом деле — нет. Чтобы разблокировать карту, человека просят прислать персональные данные, PIN-код или набрать цифры, с помощью которых активируют услугу перевода средств на чужой номер.

Запомните: никто не имеет права узнавать у вас такую информацию. И уж тем более никому вы не должны сообщать свои пароли и PIN-код. Держите его только при себе.

Воровство данных кредитных карт с помощью вирусов и троянов на компьютере.

Не устанавливайте неофициальные версии мобильных приложений.

Мошенники через Интернет или смс-сообщения распространяют вирус. И, к примеру, при попытке открыть приложение банка, вирус перенаправляет вас на сайт-ловушку, который внешне мало чем отличается от настоящего сайта банка. На этом сайте клиента просят ввести свой логин от личного кабинета. И вирус получает и отсылает мошенникам пароли для входа.

Не пользуйтесь сомнительными приложениями и регулярно обновляйте антивирусы на своих смартфонах.

Новый вид мошенничества с предложением обмена кешбэка на рубли!

Признаки мошенничества.

Злоумышленники обзванивают граждан под видом сотрудников банков и сообщают, что накопленный за покупки кешбэк и другие бонусные баллы можно обменять на рубли. Для этого мошенники запрашивают у человека банковские данные и СМС-код, полученный от банка, якобы для подтверждения операции и оплаты комиссии за услугу. Однако на самом деле злоумышленники, заполучив эти сведения, совершают кражу денег со счета.

Что предпринять?

При поступлении такого телефонного звонка прервите разговор. Сотрудники банков никогда не запрашивают по телефону финансовые данные, в том числе трехзначный код с оборотной стороны карты или СМС-код. По любым банковским вопросам, в том числе по кешбэку, самостоятельно позвоните в банк по номеру, указанному на оборотной стороне карты или на сайте кредитной организации.

КАК УБЕРЕЧЬ СЕБЯ ОТ МОШЕННИЧЕСТВА В СЕТИ.

Кибермошенничество. Правила финансовой безопасности.

Не переходите по неизвестным ссылкам, не перезванивайте по сомнительным номерам.
Если вам приходит СМС о зачислении средств (и сообщение похоже на привычное уведомление банка), а затем звонит якобы растяпа, который по ошибке зачислил вам деньги и просит вернуть, не спешите ничего возвращать.
Если вам приходит уведомление «Подтвердите покупку» и код, а следом раздается звонок опять же от «рассеянного» человека, который говорит, что по ошибке указал ваш телефонный номер, и просит продиктовать ему код, ни в коем случае не делайте этого.
Сотрудникам банка он не нужен, а мошенникам откроют доступ к вашим деньгам.
Не храните данные карт на компьютере или в смартфоне.

Установите на компьютер антивирус — и себе, и родственникам.
Проверяйте информацию. Если вам говорят, будто вы что-то выиграли или с вашей карты случайно списали деньги и нужно назвать свои данные, чтобы остановить операцию, закончите разговор и перезвоните в банк по номеру телефона, указанному на обратной стороне вашей карты.

Покупки товаров в сети.
Как не нарваться на кибермошенников.

Как защититься?

1. Проверьте реквизиты и название юридического лица.
2. Уточните, как долго существует магазин (сервис Whols).
3. Поинтересуйтесь, выдает ли магазин кассовый чек.
4. Сравните цены в разных интернет-магазинах.
5. Позвоните в справочную магазина.
6. Выясните, нет ли дополнительных оплат?
7. Не уверены в честности продавца, придерживайтесь покупок наложенным платежом.
8. Пользуйтесь маркетплейсами.

Маркетплейс - это электронная торговая площадка с большим количеством продавцов.

Известные маркетплейсы в России:

- **BERU.RU**
- **GOODS.RU**
- **OZON.RU**
- **WILDBERRIES.RU**
- **JOOM.COM/RU**

Что делать, если стали жертвой интернет-мошенников?

КИБЕРМОШЕННИЧЕСТВО В СОЦСЕТЯХ

1. Позвоните в банк и заблокируйте карту.
2. Напишите в чат банка, составьте письменное заявление или сообщите по телефону подробности мошенничества с вашей картой. Сделайте это как можно раньше.
3. Сразу обратитесь в отделение полиции по вашему адресу с заявлением о том, что стали жертвой мошенничества.
4. Обратитесь на официальный сайт МВД. Заполните формуляр, доступный на странице «Прием обращений». В строке с указанием адресата выберите «управление К МВД России».

ПОДВЕДЕМ ИТОГИ: ПРОВЕРЬТЕ СЕБЯ.

Задача 1.

Вам звонит сотрудник
Службы безопасности банка и говорит, что с вашей карты в данный момент происходит снятие денег... Ваши действия.

Задача 2

«Приведи друга, получи скидку»
Подруга рассказала о компании, которая вкладывается в информационные технологии и получает с этого доход, и что минимальный пакет акций, гарантирующий прибыль в 40%, стоит 30 000 рублей, но за каждого приведенного друга ИТ-инвесторы накидывают дополнительные 3%. У подруги так набежало почти 60% годовых, и она со дня на день ждет первой выплаты. Что предпримените?

Задача 3.

Сообщения в соцсетях о помощи.
Тебя просят положить деньги на телефон незнакомые люди. Что ты им ответишь?

Задача 4.

Пришло смс на телефон:
«Привет! Это Дима. Я пишу с чужого номера. Я потерял симку. Пожалуйста, переведи на этот номер 200 рублей. Я вечером тебе отдам».
Как вы поступите?

Советы:

Развивайте свои цифровые компетенции (навыки эффективного пользования технологиями): поиск информации, использование цифровых устройств, использование функционала социальных сетей, финансовые операции, онлайн-покупки, критическое восприятие информации, производство мультимедийного контента, синхронизация устройств.

Помните о цифровой безопасности (основы безопасности в Сети): Защита персональных данных. Надежный пароль. Легальный контент. Культура поведения. Репутация. Этика. Хранение информации. Создание резервных копий.

Развивайте и совершенствуйте свои цифровые компетенции!

Да, к сожалению преступники сумели адаптироваться достаточно быстро и в виртуальном мире, и к новым реалиям - пандемии, поэтому нам всем пользователям Интернета необходимо также оперативно научиться защищать себя от цифровых угроз. Нужно помнить, что подобные инструменты сохранят свою популярность, будут и дальше развиваться — до момента, пока общество не сможет выработать «коллективный иммунитет» к кибермошенничеству, практически, как и к Ковиду-19… А для этого необходимо реально оценивать каждую ситуацию, связанную с кибермошенничеством. Уметь противостоять всем его коварным уловкам и заманчивым предложениям.

Урядова, Н. Г. Как защититься от кибермошеничества. Правила безопасности в киберпространстве. [Электронный ресурс] : урок- предупреждение / Н. Г. Урядова ; Волжский филиал ГАПОУ «Волгоградский медицинский колледж». - Мультимедийная презентация (19 слайд). — Волжский, 2022. — USB-накопитель. — Системные требования: Windows XP или выше; ОЗУ 256 Мб; ЦПУ 500 МГц; VGA 1024x768; Установленный пакет MS Office 2003 или выше. - Загл. с экрана.