РЕГИОНАЛЬНЫЙ МАРАФОН ФИНАНСОВОЙ ГРАМОТНОСТИ

GLOBAL MONEY WEEK ПО-ЮГОРСКИ 2025

МОШЕННИЧЕСТВО В СЕТИ

КИБЕРМОШЕННИЧЕСТВО

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.

КРИПТОВАЛЮТА

Криптовалюта— это новый вид платёжного средства, предназначенный для использования в интернете. Криптовалюта не имеет физических носителей и существует только в виде программного кода. Поэтому её еще часто называют виртуальной или цифровой валютой.
Самой популярной криптовалютой является биткоин.

Мошенническая схема с криптовалютами

Махинации с криптовалютами – один из самых популярных видов
киберпреступлений. Например, сбор средств на развитие проектов в сфере криптовалют.
Мошенники могут продавать фальшивую криптовалюту за биткоин или эфириум, которые имеют реальную стоимость. После нескольких раундов сбора средств «новаторы» пропадали без вести вместе с собранными средствами
Как защититься?
Для начала изучите рынок криптовалют более детально, прежде чем вкладывать реальные деньги.

ЭЛЕКТРОННЫЕ ПЛАТЕЖНЫЕ СИСТЕМЫ

Самые популярные в России ЭПЛ:

- **ЮMoney**
- **Яндекс.Деньги**
- **QIWI**

Яндекс

Как завести электронный кошелек

- Выбрать платежную систему
- Пройти в ней несложную регистрацию
- Подтвердить свою личность

ПРАВИЛА ТЕХНИКИ БЕЗОПАСНОСТИ

1. Пройти идентификацию
2. Проводить финансовые операции только с защищенных веб-сайтов
3. Установить на компьютер или гаджет надежный антивирус
4. Использовать сложный пароль
5. Прочитать правила пользования сервисом
6. Периодически менять пароли
7. По окончании работы выходить из учетной записи

Как составить сильный пароль:

- используйте минимум 10 разных символов
- используйте заглавные и прописные буквы
- дополните Ваш пароль цифрами

БЕЗОПАСНОСТЬ В СЕТИ. БАНКОВСКАЯ КАРТА

БЕЗОПАСНОСТЬ В СЕТИ. КАК ПРЕВРАТИТЬ НАЛИЧНЫЕ ДЕНЬГИ В ЭЛЕКТРОННЫЕ?

Для этого нужно

- Завести электронное средство платежа. Что это значит? Открыть электронный кошелек или банковскую карту.
- Пополнить электронное средство платежа.

КОШЕЛЕК В СМАРТФОНЕ. Бесконтактные платежи

Мобильные зловреды

- Шпионские программы могут похищать самые разные данные — от логинов и паролей до фото и геолокационной информации, записывать звук, снимать видео, а также самостоятельно подключаться к wi-fi, чтобы передать всю собранную информацию.
- Троян Faketoken, скачанный вместе с разными приложениями, мог перехватить SMS от банка и передать его своим хозяевам, чтобы они могли совершать операции от вашего имени со своего устройства.

БЕЗОПАСНОСТЬ В СЕТИ. КАК ПРЕВРАТИТЬ НАЛИЧНЫЕ ДЕНЬГИ В ЭЛЕКТРОННЫЕ?

1. Используйте для загрузки приложений Google Play и App Store
2. Всегда устанавливайте обновления системы и приложений
3. Никогда «не светите» карту и ПИН
4. Не используйте для интернет-платежей кредитные карты или карты с овердрафтом
5. Используйте отдельную дебетовую карту для оплаты в сети
6. Подключите смс-уведомления о платежах
7. Не переходите по сомнительным ссылкам из письма или смс
8. Убедитесь, за какую точно услугу вы платите. Популярны ежемесячные оплаты
9. Если данные о карте по какой-то причине «утекли» в сеть срочно заблокируйте и оформите перевыпуск карты. Это бесплатно
10. Не уверен - не плати. Подозрительные сайты, небезопасное соединение (http:// в адресе сайта вместо https:///) – сигнал, чтобы не совершать платеж
11. Всегда используйте VPN в незнакомых местах

БЕЗОПАСНОСТЬ В СЕТИ. ПОКУПКИ ТОВАРОВ В СЕТИ

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

БЕЗОПАСНОСТЬ В СЕТИ
ЧТО ДЕЛАТЬ, ЕСЛИ СТАЛИ ЖЕРТВОЙ ИНТЕРНЕТ-МОШЕННИКОВ?

1. Позвоните в банк и заблокируйте карту

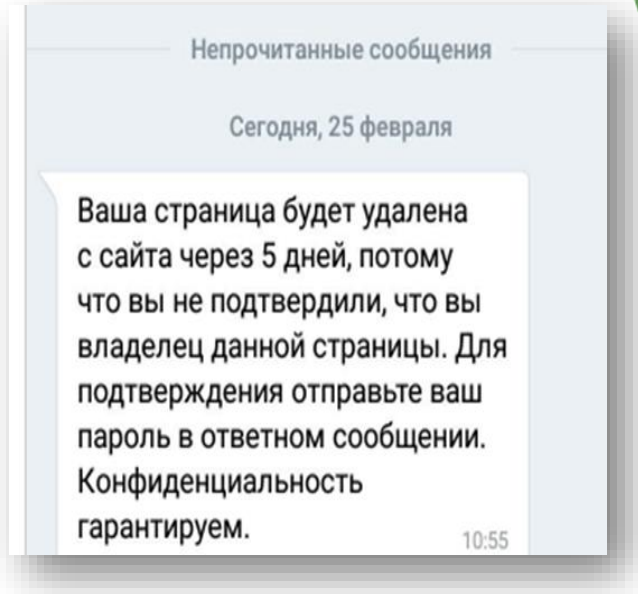
2. Напишите в чат банка, составьте письменное заявление или сообщите по телефону подробности мошенничества с вашей картой. Сделайте это как можно раньше

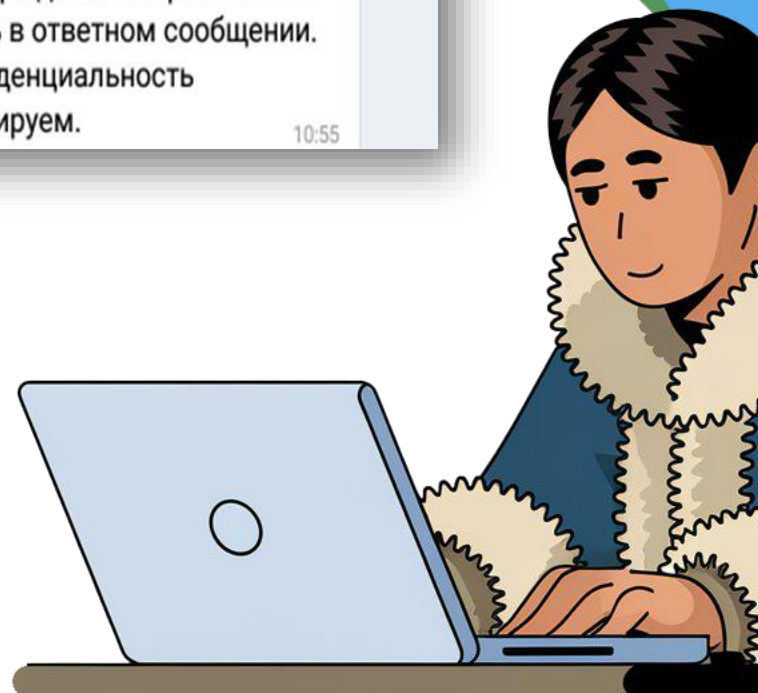
3. Сразу обратитесь в отделение полиции по вашему адресу с заявлением о том, что стали жертвой мошенничества, или

4. Обратитесь на официальный сайт МВД. Заполните формуляр, доступный на странице «Прием обращений». В строке с указанием адресата выберите «управление К МВД России».

КИБЕРМОШЕННИЧЕСТВО В СОЦСЕТЯХ
МОШЕННИЧЕСТВО ВО ВКОНТАКТЕ

1. Мнимые друзья
2. Фишинг
Фишинг (от англ. fishing — ловля рыбки) означает, что создается сайт, выглядящий точной копией другого сайта и имеющий похожий адрес (например, вконталке.ру).
3. Письмо от техподдержки
4. Письмо от банка с тестированием или розыгрышем, получение кредита
5. Отдам в хорошие руки
6. Продают и обманывают





МЕТОДЫ КИБЕРШПИОНАЖА

Фишинг: Электронные сообщения, выдающие себя за легитимные, с целью обмана пользователей и получения их данных.

Вредоносное ПО: Использование вирусов и программ-шпионов для несанкционированного доступа к системам.

Компрометация аккаунтов: Взлом учетных записей для доступа к конфиденциальной информации.

Межсетевое подслушивание: Перехват и анализ сетевого трафика для получения данных.

Физический доступ: Неавторизованный доступ к устройствам для кражи информации.

Социальная инженерия: Манипуляции и обман, чтобы убедить людей предоставить конфиденциальные данные.

СПУФИНГ АТАКИ

Что такое спуфинг атаки:

Спуфинг атаки представляют собой форму кибератак, при которой злоумышленники подделывают свою личность, данные или идентификаторы, чтобы обмануть системы, пользователей или устройства. Целью спуфинга может быть получение несанкционированного доступа к системам, кража конфиденциальных данных, введение в заблуждение пользователей или устройств, и другие.

Формы спуфинг атак:

- **Email Спуфинг:** Подделка адреса отправителя электронного письма.
- **IP Спуфинг:** Маскировка или подделка IP-адреса отправителя пакета данных.
- **Web Спуфинг:** Создание фальшивых веб-сайтов для перехвата данных или учетных записей пользователей.
- **DNS Спуфинг:** Изменение DNS-записей для перенаправления пользователей на фальшивые веб-сайты.
- **Caller ID Спуфинг:** Изменение отображаемого номера телефона при совершении звонка.
- **MAC-адрес Спуфинг:** Подмена MAC-адреса сетевого устройства для обмана сетевых систем.

BRUTE-FORCE АТАКИ

Что за атака:

Brute-force атаки — это один из наиболее простых и популярных способов взлома. Основная идея brute-force атаки заключается в попытке перебрать все возможные комбинации паролей до тех пор, пока не будет найдена правильная. Это может занять от нескольких минут до многих лет.

Типы brute-force атак:

- **Атака на пароли:** Злоумышленник перебирает различные комбинации символов, чтобы угадать пароль пользователя.
- **Атака на PIN-коды:** Например, при попытке взлома банковской карты.
- **Атака на шифрование:** Перебор ключей для расшифровки зашифрованных данных.

BRUTE-FORCE ATAKI

Утечка личной информации может привести к серьезным последствиям, включая финансовые потери и кражу личности.

Одним из способов защиты от этого является регулярная проверка утечек данных для вашего аккаунта.

Have I Been Pwned - это бесплатный онлайн-сервис, который позволяет пользователям проверить, были ли их учетные данные скомпрометированы в результате крупных утечек данных. Вы можете ввести свой адрес электронной почты или имя пользователя, чтобы узнать, был ли ваш аккаунт участвующим в каких-либо известных утечках.

Firefox Monitor - это сервис от Mozilla, который также предоставляет информацию о компрометации учетных данных. Он работает в сотрудничестве с Have I Been Pwned и предлагает аналогичные функции проверки утечек.

Google Password Checkup - это инструмент, разработанный Google, который проверяет, являются ли ваши учетные данные безопасными. Он также предупреждает вас, если ваш пароль был скомпрометирован и рекомендует изменить его.

КАК ЗАЩИТИТЬСЯ ОТ МОШЕННИКОВ?

1. Логин и пароль. Используйте сложную комбинацию из цифр и букв
2. Меняйте пароли не реже чем раз в три-четыре месяца
3. Проверяйте адрес ссылки и не вводите свой пароль от Вк на сторонних сервисах
4. Не регистрируйтесь в других соц. сетях под одним и тем же паролем
5. Проверяйте отправителя сообщения. Берегите личные данные
6. Если заходили с чужого компьютера, удалите историю посещения страниц
7. Опасайтесь сторонних приложений для скачивания музыки и видео
8. Заходите только через защищенное соединение https://vk.com/
9. Если якобы «друг» просит денег, узнайте его телефон и убедитесь, что это именно он
10. Оплачивайте товар только после получения и проверки
11. Во Вконтакте у каждого пользователя есть номер ID: https://vk.com/id… Скопируйте его и вбейте в строку поиска в разделе «Новости» — поищите информацию
12. Сообщите о мошенничестве в техподдержку Вконтакте и в банк – страницу мошенника заблокируют

МОШЕННИКИ В TELEGRAM

Бот - это сокращение от слова «робот». Бот – автономная компьютерная программа, выполняющая определенные функции.

Боты **продают различные товары или услуги** - от канцелярских ручек до автомобилей, от Деда мороза на новый год до уборки квартир.
И вот здесь нужно быть осторожным. Мошенники создают бота-клона, который копирует функционал настоящего, но после оплаты вы ничего не получите.

Как можно защититься?
Официальные телеграм-боты оставляют контакты и дают возможность связаться с представителями компании любым другим способом, кроме telegram. А ещё вход в бот должен происходить через ваш профиль на официальном сайте. А иные компании оставляют на сайте ссылку на своего бота в telegram.

Внимание! Если вам пишут личным сообщением с предложением что-то купить, то скорее всего это мошенники. А тем более, если они предлагают купить через бота. Будьте осторожны!

МОШЕННИКИ В TELEGRAM

Звонки в телеграм

Чтобы отказаться от рекламных звонков, сделайте следующее:
Приложение telegram “Настройки - Приватность и безопасность - Звонки” кто может звонить

Раскрутка канала

Есть масса чатов, где вам предложат купить рекламу в чужих каналах.

Как защититься от мошенников?

Связь с администратором любого канала и переговоры о покупке рекламы держать только через контакт, который указан в описании канала.

Телеграм-схемы заработка из даркнета

Эти схемы не работают, не тратьте деньги.

Запуски

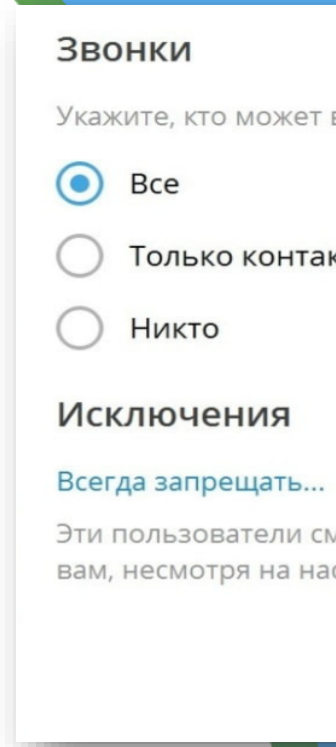
Автор объявляет о наборе учеников, инвесторов, партнёров или продажи уникального курса. После успешных продаж воздуха, канал закрывается.

Как защититься?

Прежде чем покупать инфопродукт, узнайте подробно об авторе. Забейте в поисковую строку Яндекса имя и фамилию, изучите отзывы.

КАК ЗАЩИТИТЬСЯ ОТ МОШЕННИКОВ?

1. Логин и пароль. Используйте сложную комбинацию из цифр и букв
2. Меняйте пароли не реже чем раз в три-четыре месяца
3. Проверяйте адрес ссылки и не вводите свой пароль от Вк на сторонних сервисах
4. Не регистрируйтесь в других соц. сетях под одним и тем же паролем
5. Проверяйте отправителя сообщения. Берегите личные данные
6. Если заходили с чужого компьютера, удалите историю посещения страниц
7. Опасайтесь сторонних приложений для скачивания музыки и видео
8. Заходите только через защищенное соединение https://vk.com/
9. Если якобы «друг» просит денег, узнайте его телефон и убедитесь, что это именно он
10. Оплачивайте товар только после получения и проверки
11. Во Вконтакте у каждого пользователя есть номер ID: https://vk.com/id… Скопируйте его и вбейте в строку поиска в разделе «Новости» — поищите информацию
12. Сообщите о мошенничестве в техподдержку Вконтакте и в банк – страницу мошенника заблокируют



МОШЕННИКИ В TELEGRAM

SCAM Черная метка от команды Дурова

SCAM в переводе означает "Мошенничество". Такую метку в Телеграме могут получить пользователи, каналы и боты.

Как можно пожаловаться на мошенников в Телеграме?

- Напишите в @notoscam с указанием Телеграм-ссылки на пользователя/канал/бота,
- Приложите объяснение и доказательства, почему вы считаете, что это мошенник.
- Поддержка Antiscam может задать вам уточняющие вопросы, если ваших доказательств будет недостаточно.
- Если вы увидели мошеннические действия на канале или боте, то можете переслать эти сообщения в поддержку.

СОВЕТЫ

Развивайте и улучшайте свои цифровые компетенции:

- Поиск и фильтрация информации и цифрового контента
- Анализ и критическая оценка достоверности и надежности источников данных
- Знание правил и норм поведения в социальных сетях
- Грамотно использовать функционал социальных сетей
- Производство мультимедийного контента
- Определять технические проблемы при работе и решать их
- Обеспечивать защиту устройств и цифрового контента. Знать о мерах обеспечения безопасности данных
- Работа с ботами, приложениями, покупки в сети

Изучайте цифровые финансовые продукты и услуги. Изучайте информацию и кибермошенниках и способах защиты от рисков.

! Помните о цифровой безопасности: Защита персональных данных. Защищайте пароли. Не устанавливайте ПО с неизвестных сайтов. Двухфакторная аутентификация. Осторожное использование Wi-fi в общественных местах. Не переходите по ссылкам из писем и смс от с незнакомых номеров.

ПОДВЕДЕНИЕ ИТОГОВ, ВОПРОСЫ ДЛЯ ОБСУЖДЕНИЯ

- Что Вы узнали сегодня нового?
- Какие покупки Вы чаще всего совершаете онлайн?
- Каким маркетплейсом пользуетесь?
- Кто такие финансовые кибермошенники?
- Какие вы узнали виды мошенничества в соцсетях?
- Как можно себя обезопасить в интернете?
- Что такое метка SCAM и почему на нее надо обращать внимание?
- Вы общались в сети с чат-ботом?
- Что Вы расскажете своим родителям и друзьям об этом уроке?

РЕШЕНИЕ ЗАДАЧ

Задача 1.
Звонок по телефону: «Добрый день. Это Банк «Ваш банк». Только что мы засекли подозрительную попытку списания с вашей карты 3000 рублей. Если это были не вы, то вам нужно подтвердить ваши данные, чтобы в будущем злоумышленники не смогли списать ваши деньги. Продиктуйте пожалуйста, смс-код, который направлен вам на телефон». Ваши действия?
Задача 2.
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?
Задачи 3.
В популярной соцсети вам пришло сообщение от инвестиционной компании с предложением инвестировать деньги в новые акции «VVV – инвест». Первоначальный взнос составляет всего 10000 рублей. Гарантированная прибыль от 40% годовых. Приложены скрины, подтверждающие получение выплат и отзывы людей: как хорошо, что они инвестировали деньги в эти акции, теперь прекрасно живут.
Ваши действия?

ЗАДАНИЯ

1. Расскажите своему напарнику о самых полезных приложениях в телефоне, которые вы используете? Чем конкретно они полезны? А также назовите самое бесполезное приложение, которое вы не советуете скачивать.

2. Устройте дискуссию с друзьями на тему «Можно ли победить финансовую киберпреступность, создав суперкомпьютер?»

СПАСИБО ЗА ВНИМАНИЕ!