

РЕГИОНАЛЬНЫЙ МАРАФОН ФИНАНСОВОЙ ГРАМОТНОСТИ

GLOBAL MONEY WEEK ПО-ЮГОРСКИ 2025



ВИРТУАЛЬНЫЕ
ЛОВУШКИ, ИЛИ КАК
НЕ ПОТЕРЯТЬ ДЕНЬГИ
ПРИ РАБОТЕ В СЕТИ
ИНТЕРНЕТ

ИНТЕРНЕТ: НЕ ТОЛЬКО БЛАГО, НО И ОПАСНОСТЬ

Сеть Интернет не только помогает нам общаться и работать, но и стала местом действия мошенников, желающих завладеть нашими деньгами и личными данными

Попробуйте определить, на какой из предложенных интернет страниц деньги пользователя рискуют оказаться в руках мошенников?

- <https://online.sberbank.ru/CSAFront/index.do>
- <http://sberbank-online1.ru/>
- <http://www.superkopilka.com>

Давайте узнаем, как не попасть в их ловушки

ФИШИНГ – САЙТЫ-ОБМАНКИ

Фишинг — это способ мошенничества, при котором поддельный сайт выглядит как настоящий (например, сайт банка или интернет-магазина). Невнимательный пользователь вводит свои данные и теряет деньги

Как распознать?

- Смотрите на адрес сайта. Даже одна неправильная буква должна вызвать подозрение

Как защититься?

- Всегда проверяйте, чтобы адрес начинался с <https://>, и не переходите по подозрительным ссылкам в письмах и сообщениях





ФАРМИНГ – СКРЫТЫЙ ВРАГ

Фарминг опаснее фишинга. Здесь компьютер заражается вирусом, и даже правильный адрес сайта может привести на мошеннический ресурс

Как происходит?

- Вы незаметно для себя попадаете на поддельные страницы. Смотрите на адрес сайта. Даже одна неправильная буква должна вызвать подозрение

Что делать?

- Используйте хороший антивирус, который своевременно остановит угрозу



СКАНДИНАВСКИЙ АУКЦИОН – ИГРА, В КОТОРОЙ СЛОЖНО ВЫИГРАТЬ

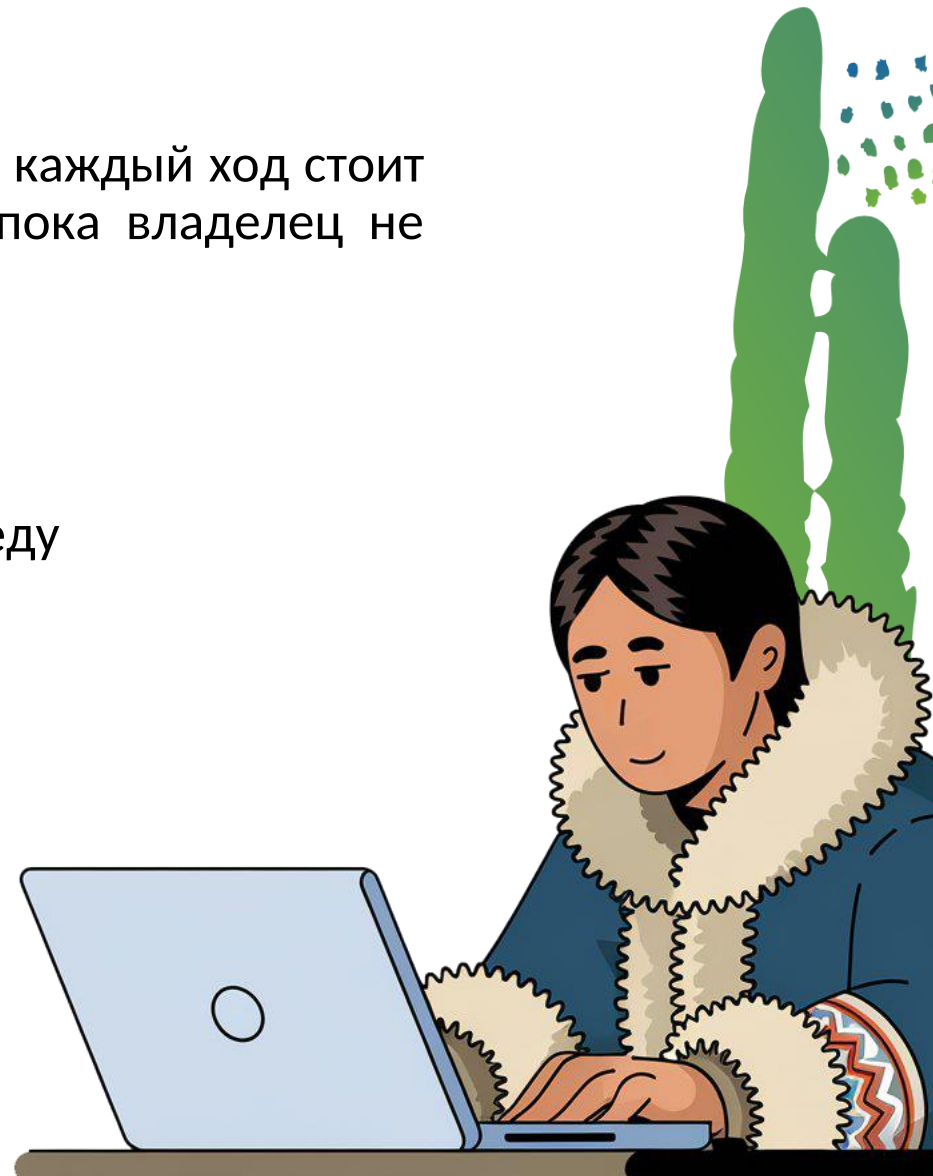
На первый взгляд, это просто аукцион с низкими ставками. Но каждый ход стоит денег, а специальные роботы повышают цену до тех пор, пока владелец не получит достаточный доход

В чём опасность?

- Ваши деньги уходят на бесконечные ставки, шансы на победу малы

Совет?

- Подумайте дважды, прежде чем участвовать





EVIL TWIN (ЗЛОЙ ДВОЙНИК) – WI-FI ЛОВУШКА

Мошенники создают поддельные Wi-Fi сети, чтобы похищать данные пользователей

Что происходит?

- Вы подключаетесь к бесплатному Wi-Fi, и все ваши данные попадают к мошенникам

Как избежать?

- Подключайтесь только к проверенным сетям и отключите автоматическое подключение к неизвестным точкам





НИГЕРИЙСКОЕ ПИСЬМО – ОБЕЩАНИЕ БЫСТРОГО БОГАТСТВА

Вам приходит письмо с обещанием крупных сумм или наследства. Чтобы получить деньги, нужно оплатить «небольшой» сбор. Конечно, никаких денег после этого вы не увидите

Как быть?

- Не реагируйте на такие сообщения и сразу помечайте их как спам





«СЕМЬ КОШЕЛЬКОВ» – ПРОСТАЯ, НО ОПАСНАЯ СХЕМА

Мошенники предлагают схему быстрого заработка: нужно перевести небольшие суммы на чужие кошельки и ждать больших денег

Почему это опасно?

- Это финансовая пирамида, в которой заработать невозможно. Вы только потеряете свои деньги

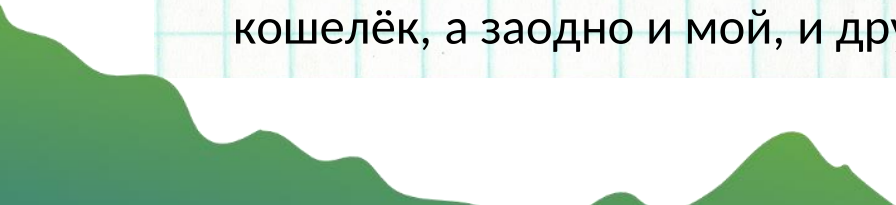
Совет?

- Не верьте обещаниям лёгких денег в сети





«Я предлагаю вам возможность зарабатывать деньги, не выходя из дома, участвуя в проекте от организаторов системы «Деньги». После первых 2–3 мес. участия в данном проекте вы будете иметь доход не менее 1 тыс. долл. в месяц, это доказано многочисленными участниками проекта. Ваш доход будет полностью зависеть от ваших усилий и времени, затраченного на работу. Никакого подвоха. Вам всего лишь придётся потратить 90 руб., и вы начнёте работать. Работа в основном заключается в размещении объявлений на специализированных сайтах. Для получения солидного дохода вам нужно ежедневно размещать сотню объявлений, проходя регистрацию на многих сайтах. также нужно отвечать на письма. Потребуется усердие и время. Суть проекта «Деньги». Вы получаете список из 7 номеров, каждый номер — это кошелёк одной из платёжных систем одного из участников проекта. Для вступления в проект вы переводите с вашего кошелька по 10 руб. на каждый кошелёк из списка. затем сдвигаете номера в списке на одну позицию вверх. В результате верхний (первый) номер удаляется из списка (и выбывает из проекта) и высвобождается нижняя (седьмая) позиция в списке. В эту (седьмую) позицию вы вписываете номер вашего кошелька. теперь ваш кошелёк в списке кошельков участников проекта! Приступаете к работе. Размещаете своё объявление в сети Интернет, на сайтах, посвящённых поиску работы, тем самым распространяете список, содержащий ваш кошелёк, а заодно и мой, и других участников проекта»





ФИНАНСОВЫЕ ПИРАМИДЫ И ХАЙПЫ

Хайпы (HYIP) обещают быстрый и высокий доход за короткий срок. На самом деле это финансовые пирамиды, которые скоро рухнут, а вкладчики потеряют деньги

Чем опасно?

- Никто не вернёт вам деньги, если пирамида рухнет

Как защититься?

- Избегайте сомнительных инвестиционных проектов с фантастическими обещаниями



КАК ЗАЩИТИТЬСЯ?

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. Заходите только через защищенное соединение <https://vk.com/>
8. Если якобы «друг» просит денег, узнайте его телефон и убедитесь, что это именно он
9. Оплачивайте товар только после получения и проверки
10. Во Вконтакте у каждого пользователя есть номер ID: <https://vk.com/id...> Скопируйте его и вбейте в строку поиска в разделе «Новости» — поищите информацию
11. Сообщите о мошенничестве в техподдержку Вконтакте и в банк — страницу мошенника заблокируют

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



СОВЕТЫ

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

ЗАДАНИЕ 1

Опишите известные вам виды интернет-мошенничества, которые не были рассмотрены в рамках данного занятия. Для описания используйте приведённый ниже план:

1. Суть мошенничества.
2. Причина распространённости данного вида мошенничества.
3. Способ защиты от мошенничества



ЗАДАНИЕ 2

Какие советы не смогут уберечь вас от фишинга?

Найдите верные ответы.

1. Важно внимательно изучить адрес сайта в адресной строке.
2. Необходимо переходить по всем ссылкам, всплывающим на интернет-страницах.
3. Пользователь должен остерегаться перехода по спамовым рассылкам со взломанных страниц.