**Единый классный час «Осторожно киберпространство»**

**Подготовила и провела Горожанина З.А.**

1.Познакомить обучающихся с преимуществами сети Интернет, скрытыми и открытыми угрозами Интернета, классификации интернет угроз;

2. Сформировать понятия Интернета;

3. Научить обучающихся критически относиться к информационной продукции, распространяемой в сети Интернет;

4. Уметь отличать достоверные сведения от недостоверных, вредную информацию от безопасной;

**5. Распознавать признаки злоупотребления неопытностью и доверчивостью обучающихся,**

**попытки вовлечения их в противоправную деятельность**

**Ход занятия**

<https://www.youtube.com/watch?time_continue=235&v=FKHMu9Ckqds> и видиоматериалов в телефоне о случаях мошенничества.

2000 по 2004 год обычно принято считать началом современного этапа развития компьютерной «инфекции». К началу нового тысячелетия вредоносные компьютерные программы и их авторы превратились в одну из самых масштабных проблем не только для профессиональных программистов, пользователей и компьютерного сообщества. Они стали непрекращающейся «головной болью» всего мирового сообщества, так как наносимый ими моральный и материальный ущерб личности, ведущим отраслям современного промышленного производства, сфере услуг, банковским структурам, государственным органам управления и обществу в целом достиг недопустимых размеров

**Ответе на вопросы: Что такое?**

**Фишинг** (phishing) – вид интернет-мошенничества, использующий принципы социальной инженерии. Это письмо в электронной почте, звонок, SMS или сообщение в мессенджере или соц.сети, пытающееся обманом убедить пользователя передать свои конфиденциальные данные, скачать какой-то вредоносный файл или перевести деньги. Для этого отправитель представляется неким другим лицом, от которого подобная просьба вызывает меньше подозрений.

**Скаммер** (англ. *scam*, мошенничество) — мошенник, который занимается сбором личных сведений о пользователях, посредством их использования в корыстных целях, чаще всего — получения денежной помощи, или подарков, путем ввода жертвы в трансовое состояние, с использованием хитрых технологий НЛП.

**Вишинг?**

*Vishing* (voice phishing, голосовой фишинг) — это вид атаки, при котором жертву пытаются убедить раскрыть ценную личную информацию по телефону. Хотя по описанию это похоже на старый добрый скам, вишинг-атаки имеют элементы хай-тека: например, в них применяется технология автоматизированной симуляции голоса, или для упрощения задачи скаммер может использовать персональную информацию о жертве, собранную во время предыдущих кибератак.

«**Смишинг**» (smishing) — это похожий тип атак, при котором вместо электронной почты или голосовых звонков используются текстовые сообщения;

Псевдоинвестиции - это проекты, созданные для заработка мошенников на доверчивости людей. Также псевдоинвестиции называют **Хайпами**

**“Волшебные” кошельки и Киви-ваучеры.**

Есть миф, в котором говорится, что существуют некие волшебные кошельки, “на который отправишь 100,01 рублей, а придет 200,02”. А Киви-ваучеры - способ передачи этих самых денег в платежной системе Visa Qiwi. Запомните! Не существует и не может существовать никаких волшебных кошельков. Это никому не выгодно.

“Вы выиграли айфон, отправьте 500 рублей на номер 8-924-356-72-35 за доставку и телефон ваш!” Именно в таком стиле к вам могут приходить SMS, электронные письма, “выскакивать” реклама на сайтах и т.п. На такие письма не стоит даже обращать внимание, кроме тех случаев, в которых в лотерее или конкурсе вы реально участвовали по собственной инициативе.

Мошенники могут под видом «честных» людей рассказывать о кошельках, которые якобы принадлежат каким-то мошенникам. Вам предлагается разорить их «умножением денег», отомстить за то, что они кого-то обманывают.

Шумиха, ажиотаж, крикливая реклама и в том числе обман). Основные признаки хайпа - высокий процент. Многие хайпы предлагают огромный процент, от 3,5% в день, что больше, чем 100% в месяц. Думаю, многие понимают, что такой заработок нереален. Второй признак - отсутствие реальных контактных данных. Они либо ненастоящие, либо их попросту нет.

Теперь поговорим о механике работы хайпа. На главной странице сайта написано, чем проект якобы занимается и якобы почему проект приносит такие доходы. Это могут быть продажи нефти, поиск звезд или вообще что угодно. Мы платим, к нам должен приходить процент. На самом деле эти проекты ничего не производят, так откуда у них деньги? Все просто. В проект приходят новые люди, вносят свой депозит. Вам дают процент. Если проект больше не платит или сайт вообще исчез, это называется **скам** (от англ. scam — мошенничество).

Список можно продолжить, но надо знать, что в интернете мошенничество происходит чаще всего под такими предлогами:

1. Заработок.
2. Помощь страждущим.
3. Разблокировка опций программ, приложений.
4. Выгодное приобретение товаров.
5. Розыгрыш ценных призов.

Бессмыслица, но и подобным историям кто-то верит, а в результате сам оказывается обманутым. На самом деле никогда не существовало каких-либо секретных счетов, возвращающих вам средства в увеличенном виде. А владельцы кошельков – это сами авторы подобных историй. Они просто стараются привлечь внимание и заставить людей перевести на свои счета деньги.

**Почти все «волшебные» кошельки располагаются в системе Яндекс .**

**Суперпрограммы, суперзадачки** для быстрого заработка.

Один из самых известных видов мошенничества. Вы покупаете какую-то программку, доступ на сайт или что-то подобное, решаете простые примеры или что-то подобное и зарабатываете деньги. Якобы зарабатываете. Думаете, вы получите заработанные деньги? Нет! Вы не получите ничего.

**Не стать жертвой финансовых махинаций можно, для этого нужно просто выполнять определённые правила и применять меры безопасности.**

* Прежде чем выходить в Интернет, установите на компьютер хорошую антивирусную программу. Следите за тем, чтобы антивирусные базы все время были актуальными, и помните, что в мире ежечасно появляется несколько новых вирусов.
* Будьте максимально бдительны и осторожны при посещении неизвестных страниц в Интернете. Сегодня широко распространены шпионы и вирусы, для заражения которыми достаточно просто зайти на определенную веб-страницу.
* После скачивания из Интернета файлов, архивов и т. п. надо сразу же проверить их антивирусной программой, и только после этого запускать на выполнение, распаковывать и т. д. Помните, что многие вредоносные программы распространяются в виде исполняемых файлов либо архивов.
* Старайтесь не открывать сайты платежных систем по ссылке (например, в письмах). Обязательно проверяйте, какой url (адрес, указывающий путь к интернет ресурсу, на котором размещены различные виды файлов) стоит в адресной строке или посмотрите в свойствах ссылки, куда она ведет. Вы можете попасть на сайт-обманку, внешне очень похожий, практически неотличимый от сайта платежной системы. Расчет в этом случае на то, что вы введете на таком сайте свои данные, и они станут известны мошенникам.
* Никогда никому не сообщайте ваши пароли. Вводить пароли можно и нужно только на сайтах самих платежных систем, но никак не на других ресурсах. Избегай стандартных паролей! Многие пользователи часто совершают одну и ту же ошибку, пользуясь стандартными, шаблонными паролями. Один из самых характерных примеров – когда пароль совпадает с логином. Подобрать такой пароль элементарно, а дальше злоумышленник будет действовать в зависимости от того, к чему относится данный пароль. Если это кредитная карта или банковский счет, управлять которым можно через Интернет – все деньги с этого счета исчезнут моментально.
* Если при посещении различных ресурсов в Интернете (форумы, страницы регистрации, и т. д.) требуется оставить о себе некоторые данные, то они должны содержать минимум сведений. В частности, никогда и никому не сообщайте свои паспортные данные, домашний адрес, различные пароли и т. п. Несмотря на то, что владельцы и руководители многих Интернет-ресурсов гарантируют полную конфиденциальность, не будьте наивными: если кому-то надо получить эту информацию, он ее получит, и вполне может использовать для шантажа, вымогательства и т. п.
* Не храните файлы с секретной информацией на доступных или недостаточно надежных носителях информации. Всегда делайте несколько копий таких файлов на разных носителях.
* Если вам предлагают удаленную работу и при этом просят оплатить регистрационный взнос, в качестве гарантии, за пересылку данных и тому подобное — 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. В любом случае, обоснование платежа значения не имеет – важно помнить одно: если в любом поступившем из Интернета предложении, рекламе и т. п. содержится требование или просьба перевести деньги – это однозначно мошенничество.
* 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 глядя. Техническая поддержка платежных систем никогда не рассылает таких писем.
* Не давайте деньги в кредит неизвестным вам лицам - в интернете не существует гарантий возврата кредитов.
* В 99% случаев платежи, которые вы делаете онлайн, отменить нельзя. Поэтому семь раз подумайте, прежде чем один раз оплатить товар или услугу

Помимо перечисленных правил безопасности, при работе в Интернете руководствуйтесь нормами и принципами, которые диктуется здравым смыслом и элементарной осторожностью.

