Автор (ФИО, образовательное учреждение):	Юшкевич Ольга Григорьевна заведующая библиотекой МАОУ гимназия №7 «Сибирская»
Название модуля и тема внутри модуля (ненужное удалить):	**Модуль 4. Цифровое потребление** ● Мошенничество в сети
Форма (ненужное удалить):	выступление перед коллегами
Класс:	коллеги
Тема урока (собрания, выступления и т.д.):	«Мошенничество в сфере Интернета»
Цель:	Познакомить коллег с видами мошенничества в Интернете
Основные вопросы	Виды мошенничества
Необходимые материалы:	
Дополнительные материалы по теме:	видео-ролик https://www.youtube.com/watch?v=qjwbcZN0XLI https://www.youtube.com/watch?v=TwqqSbBbe90

Что делает среднестатистический пользователь в Интернете? Ищет информацию, скачивает музыку и фильмы, пишет в блог, посещает развлекательные сайты, пользуется почтой и т.п. Но вот однажды он сталкивается с заманчивым предложением заработать энную сумму денег за короткое время. Неважно, что именно ему предлагают, в его голове уже начинают крутиться мысли о легком заработке. Даже если он достаточно осторожен и не доверяет всему, что пишут, качественный дизайн и грамотный текст могут развеять все его сомнения. Что уж говорить о неопытных подростках… Человек отсылает нужную сумму на кошелек или проводит какие-то другие действия, и терпеливо ждет. Мошенник же получает свои деньги.

Мошенничество в Интернете приобретает все большие масштабы. Изобретаются все новые уловки по выкачиванию денег с простодушных пользователей. Практически полная безнаказанность, анонимность мошенников, большое количество доверчивых людей – все это подпитывает такой вот своеобразный вид ‘бизнеса’.

Большинство пользователей просто забывают о том, что в Интернете действуют те же законы, что и в жизни. Сейчас редко найдешь человека, который бы попытался выиграть у наперсточника на вокзальной площади, а вот когда ему же предложат отослать деньги на так называемый ‘волшебный’ кошелек, с тем, чтобы потом получить удвоенную сумму, все защитные психологические барьеры вдруг оказываются снятыми, и он с радостью соглашается. Все это напоминает 90-е годы, когда люди только после своего горького опыта (и чаще неоднократного) становились более осторожными, встречаясь с очередным предложением ‘легких’ денег. В Интернете, как мы видим, ‘90-е’ в самом разгаре…

Главное, что нужно помнить всем - ‘халявы’ не бывает. Никто никогда не даст денег просто так. Деньги не появляются из неоткуда, даже если они ‘электронные’. А Интернет – это просто средство передачи информации .Как известно, средствами получения денег является либо производство товаров, либо предоставление услуг. Для Интернета данное утверждение звучит так: либо вы получаете прибыль с производства интеллектуальной собственности, либо с предоставления сопутствующих услуг....

Виды мошенничества

1. **Мошенничества, связанные с Интернет-магазинами.**

Через Интернет вам могут предложить приобрести все, что угодно, а распознать подделку при покупке через сеть бывает сложно. Однако, соблюдая некоторые правила покупки товаров через Интернет, можно оградить себя от возможных неприятностей.

Вас должна насторожить слишком низкая цена на определенный товар, а также отсутствие фактического адреса или телефона продавца. Скорее всего, вам предлагают приобрести подделку либо хотят присвоить ваши деньги.

Не поленитесь позвонить продавцу по телефону и подробнее выяснить уже известные вам особенности товара, его технические характеристики и т.д. Заминки на другом конце провода или неверная информация, которую вам сообщили, должны стать поводом для отказа от покупки в данном Интернет-магазине.

Наведите справки о продавце, изучите отзывы о его работе, и только после этого решайте - иметь ли дело с выбранным вами Интернет-магазином.

Пользуйтесь услугами курьерской доставки и оплачивайте стоимость товара по факту доставки.

2. Фишинг

Фишинг (от англ. fishing - рыбная ловля, выуживание) - вид интернет-мошенничества, цель которого - получить данные, содержащиеся на вашей пластиковой карте.

Злоумышленники рассылают электронные письма от имени банков или платежных систем. Пользователю предлагается зайти на сайт, который является точной копией настоящего сайта банка, где можно увидеть объявления, например, об изменении системы безопасности банка. Для дальнейшей возможности использовать свою пластиковую карту вас просят указать пин-код и данные, содержащиеся на карте. Впоследствии эти данные используются для изготовления поддельной пластиковой карты и обналичивания денежных средств, содержащихся на вашем счете. Оставив свои данные, вы фактически преподносите мошенникам деньги на блюдечке.

Одной из разновидностью данного вида правонарушения являются звонки на сотовые телефоны граждан якобы от представителей банка с просьбой погасить задолженность по кредиту. Когда гражданин сообщает, что никакого кредита не брал, ему предлагается уточнить данные, содержащиеся на пластиковой карте. Этого уже достаточно для покупки товаров в Интернет-магазинах.

Следует помнить, что банки и платежные системы никогда не присылают писем и не звонят на телефоны граждан с просьбой предоставить

свои данные. Если такая ситуация произойдет, вас попросят приехать в банк лично.

3. Интернет-попрошайничество

В Интернете могут появиться объявления от благотворительной организации, детского дома, приюта с просьбой о материальной помощи больным детям. Злоумышленники создают сайт-дублер, который является точной копией настоящего, меняют реквизиты для перечисления денег.

Для того, чтобы не попасться на крючок и не отдать свои деньги в руки мошенников, не поленитесь перезвонить в указанную организацию, уточнить номер расчетного счета либо посетить ее лично, убедиться в достоверности размещенной информации, выяснить все подробности дела, а затем уже решать - передавать деньги или нет.

4. Мошенничества в отношении иностранных граждан (брачные аферы).

Не встретив в реальной жизни свою половину, многие мужчины продолжают искать ее в Интернете. Поиски начинаются на сайтах знакомств и дневниках, где будущие избранницы размещают свои фотографии.

Этим пользуются злоумышленники, используя фото девушек, привлекая психологов, программистов, переводчиков и посредством этих сайтов завязывают переписку с доверчивыми иностранцами.

Западные женихи «клюют» на объявления, где нетребовательные русские красавицы говорят о том, что нуждаются в серьезных отношениях. А взамен вечной любви, порой после месяцев переписки, просят решить их финансовые проблемы - помочь обеспечить сиделкой больных родителей, расплатиться с кредитом, перевести деньги на перелет к жениху в дальнее зарубежье и т.д.

После получения денег невесты перестают выходить на связь. Пылкие иностранные поклонники, поняв, что их обманули, обращаются в полицию. Злоумышленники рассчитывают только на женихов из дальнего зарубежья, т.к. представители ближнего зарубежья предпочитают приехать в гости к невесте сами, что невыгодно для мошенников.

5. Осторожно!!!!! Вирус!!!!!

Сущность вируса - переадресация со страницы запрашиваемого ресурса на фиктивную, скопированную с настоящей. Подмена осуществлялась для самых популярных ресурсов Рунета: Яндекс, Рамблер, Майл, ВКонтакте, Одноклассники.

Набирая на «зараженном» компьютере адрес одного из указанных ресурсов, пользователь попадает на сервер-подмену, где ему предлагается страница для входа в систему (имя и пароль). С учетом того, что в адресной строке указано корректное имя, а внешний вид скопирован с оригинального сервера, у большинства пользователей не возникает подозрений в подлинности страницы.

После ввода имени и пароля отображается иная страница, где уже говорится о необходимости «подтверждения» или «активации» учетной записи за смс на короткий номер, стоимость которого минимальная или якобы бесплатная.

Таким образом, злоумышленники не только снимают денежные средства со счетов абонентов, но и получают логин и пароль доступа пользователя к указанным популярным ресурсам, что позволяет им в дальнейшем отправлять от имени «жертвы» различные сообщения, например:

- программка для бесплатной отправки подарков! - http://re-url.me/abc , мне не забудь отправить!

- привет. http://www.894.joo.ru Лови программку по бесплатному повышению рейтинга, но не давай никому больше. Это не спам.

Основные темы, которые используются для «рекламы» скачивания и запуска зараженных программ:

- бесплатное повышение рейтинга «В Контакте»;

- программа перехвата SMS сообщений с телефона;

- дополнительные функции в социальных сетях, которые не существуют (подарки, VIP-доступ и т.д.)

После перехода по ссылке компьютер пользователя автоматически запускает вредоносную программу

Наши рекомендации

Пострадавшим рекомендуется изменить пароль доступа к указанным ресурсам, а также установить версии антивирусных программ с обновленными антивирусными базами.

Следует помнить, что ресурсы популярных сайтов никогда не потребуют от уже зарегистрировавшегося пользователя дополнительной авторизации, тем более за деньги путем отправки смс.

Смотрим видео-ролики «Мошенничество в интернете»

https://www.youtube.com/watch?v=qjwbcZN0XLI
https://www.youtube.com/watch?v=TwqqSbBbe90