Муниципальное бюджетное общеобразовательное учреждение

«Средняя общеобразовательная школа №15 с. Бада»

ИНФОРМАЦИОННЫЙ ПРОЕКТ

МОШЕННИЧЕСТВО В ИНТЕРНЕТЕ

Автор:

Шильников Руслан Алексеевич

обучающийся 10 А класса

Руководитель работы:

Яковлев Михаил Павлович, учитель ОБЗР.

С. Бада

2025 год

Оглавление

Введение

В современном мире интернет стал неотъемлемой частью жизни, особенно для молодежи. Это глобальное информационное пространство предоставляет учащимся доступ к огромному количеству знаний и ресурсов, однако оно также связано с определенными рисками и опасностями: злые люди, которые хотят получить выгоду, могут обмануть нас. Поэтому нужно быть осторожным в интернете.

В рамках данного проекта я постараюсь выяснить, что нужно знать о мошенничестве, как защитить себя от мошенников и уметь их избегать.

Проблемой моего проекта является информированность учеников школы «МБОУ СОШ №15 с. Бада» об интернет мошенничестве, которая находится на невысоком уровне.

Актуальность проблемы: в наше время мы проводим все больше времени в Интернете, где осуществляется немалая часть нашей работы, а также хранится множество информации и поддерживается связь с людьми. Поиск информации в сети стал для нас обыденным делом, а онлайн-покупки вошли в повседневную практику. Однако параллельно с этим растет и количество интернет-мошенничества, при этом информированность учеников находится на крайне малом уровне, поэтому я считаю, что эта проблема остается крайне важной в современном обществе.

Цель: ознакомить учеников МБОУ СОШ № 15 с. Бада со схемами мошенничества, методами борьбы и противостояния им.

Задачи:

- Рассмотреть историю появления мошенничества.
- Рассмотреть основные способы мошенничества.
- Рассмотреть способы борьбы с мошенничеством.
- Провести опрос среди учеников нашей школы и выяснить хорошо ли они проинформированы о мошенничестве в интернете.
- Создать рекомендации по безопасному использованию сети Интернет.

Теоретическая часть

Кибер-мошенничество: что это такое и какими они бывают.

Понятие кибер-мошенничества:

Кибер-мошенничество — это обман, осуществляемый с использованием компьютеров и интернет-технологий. Оно может принимать различные формы, от простого мошенничества через электронную почту до сложных схем, основанных на социальном инжиниринге. Также к киберпреступности, кроме мошенничества, относятся кража личных данных с последующим кибер-преследованием. (1)

Исторический контекст:

Кибер-мошенничество начало развиваться с ростом популярности интернета еще в 1990-х годах. Появление мобильных телефонов с выходом в интернет упростило труд мошенников. Самым популярным способом была история о ДТП, с помощью которой происходило вымогательство денежных средств у родственников. С тех пор схемы обмана эволюционировали, и мошенники используют все более сложные технологии для обмана пользователей. Например, создание уникальных вредоносных программ, которые в считанные секунды могут обнулить счет пользователя интернета. (2)

Законы и подзаконные нормативные правовые акты субъектов Российской Федерации:

Государство старается регулировать деятельность в сфере интернет-безопасности, защищая права граждан, наказывая злоумышленников и предотвращая акты мошенничества с помощью следующих законов:

Федеральный закон от 28 декабря 2010 г. N 390-ФЗ «О безопасности» закрепляет правовые основы обеспечения безопасности личности, общества и государства, определяет систему безопасности и ее функции, устанавливает порядок организации и финансирования органов обеспечения безопасности, а также контроля и надзора за законностью их деятельности. Закон определяет ключевые термины в области безопасности, которые применимы и для сферы информационной безопасности, принципы и систему безопасности, правовой статус и состав Совета Безопасности Российской Федерации.

Федеральный закон от 27.07.2006, г., № 149-ФЗ «Об информации, информационных технологиях и о защите информации» фиксирует базовые нормы для всей системы информационного законодательства, в т.ч.

правового обеспечения информационной безопасности. Они определяют основные термины и их определения, принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации (ст.3), классификацию информации по категориям доступа - общедоступную и ограниченного доступа (ст. 5), порядку ее предоставления или распространения (свободно распространяемую, обязательного предоставления или распространения, ограниченного распространения или запрещаемую для распространения вообще). Закон определяет базовые положения правового режима доступа к информации (ст.8) и его ограничения (ст.9), основные параметры правовых режимов распространения (ст.10) и документирования (ст.11) информации, информационных систем (ст.13), информационно-телекоммуникационных сетей (ст.15) и общие условия защиты информации (ст.16), информационных систем (ст.13) и использования информационных технологий, а также в общих чертах описывает ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.

Уголовный кодекс РФ в главе 28 Кодекса предусматривает ответственность за совершение преступлений в сфере компьютерной информации (ст.272-275). Всего в тексте Кодекса содержится более 50 отдельных статей, устанавливающих уголовную ответственность за нарушение установленных запретов в информационной сфере.

Виды кибер-мошенничества и как бороться с ними.

Однако несмотря на преследование законом, кибер-аферисты продолжают свое развитие, и в наше время, несомненно, стало значительно больше разнообразных видов бесконтактного мошенничества.

Мошенничество с предложением работы.

Во время пандемии COVID-19, когда миллионы людей в связи с карантином искали удаленную работу через интернет, мошенники стали использовать новый способ обмана, который процветает и в наши дни. Они отправляют электронное письмо с предложением работы. Например, вам могут предложить стать «тайным покупателем».

Если вы согласитесь, вам выдают чек или платёжное поручение на сумму больше, чем договаривались. Потом вас просят вернуть разницу. Но чек или платёжное поручение окажутся поддельными, и вы потеряете деньги.

Чтобы не попасться на эту уловку, не обналичивайте подозрительные чеки, пока не убедитесь, что они настоящие. Для этого попросите свой банк заморозить средства до подтверждения подлинности чека или платёжного поручения. Если вас просят вернуть разницу, это значит, что вы имеете дело с мошенником.

Мошенничество с лотереей.

По данным, в 2020 году мошенничество с лотереей стало четвёртым по популярности видом мошенничества.

Вам приходит электронное письмо с сообщением, что вы выиграли крупную сумму в неизвестной лотерее, обычно в другой стране. Для получения выигрыша вам предлагают заплатить деньги. Обычно мошенники утверждают, что это страховой сбор, подоходный налог, банковская комиссия или оплата услуг курьерской доставки.

Вас также могут попросить предоставить данные для подтверждения вашей личности, и вы становитесь жертвой кражи персональных данных, а ваши деньги пропадают.

Есть ещё один вариант этой схемы: мошенник получает доступ к аккаунту жертвы в социальных сетях, связывается с её друзьями и родственниками и сообщает им, что все они выиграли деньги. Потом он присылает адрес электронной почты для получения инструкций о том, как получить выигрыш. Это особенно коварная схема, потому что мошенник спекулирует на доверии между друзьями и членами семьи, чтобы выманить у них деньги.

Чтобы не подвергнуть себя обману, проверьте, кто отправил письмо. Если это физическое лицо, а не компания, и вы не единственный в списке адресатов, и вы впервые слышите об этой лотерее, это может быть мошенничество.

Мошенничество с переводом денег.

Вам поступает смс или звонок от человека, которому нужно срочно перевести деньги. Иногда отправитель выдаёт себя за знакомого или друга, но чаще всего он представляется членом вашей семьи (братом, сестрой или мамой с папой), которому срочно понадобились деньги или он может сказать, что попал в какое-либо происшествие и попросит перевести ему

деньги. В письме или звонке содержится ровно столько информации, сколько нужно, чтобы предложение выглядело правдоподобно

Но перевод денег неизбежно откладывается, а вы уже на крючке и вынуждены совершать множество мелких платежей якобы для ускорения вывода денег.

Важно: обратите внимание на информацию, содержащуюся в предложении. Если оно содержит орфографические и грамматические ошибки, а адрес для ответа не совпадает с адресом отправителя, это может быть мошенничество.

Мошеннические сообщения и звонки.

Мошенники применяют разнообразные методы, чтобы ввести людей в заблуждение и завладеть их денежными средствами. Они используют различные каналы коммуникации, такие как SMS, telegram, VK, WhatsApp, Facebook Messenger, Viber или Skype.

Вот несколько примеров мошеннических действий:

• Вам приходит сообщение о том, что вам отправлена посылка, но для её получения необходимо подтвердить свою личность или оплатить доставку.

• Вам пишут, что ваш счёт будет закрыт или карта заблокирована, и вам грозит штраф. Чтобы избежать этого, необходимо подтвердить свой аккаунт на поддельном сайте.

• Вам сообщают о крупном выигрыше, но для его получения необходимо предоставить свои данные для оплаты.

Мошенничество в интернет пространстве.

Мошенничество с банковскими картами по телефону – наиболее действенный способ получить средства с чужой банковской карты. Злоумышленник представляется «сотрудником» банка с целью узнать данные вашей карты.

Подобные запросы банки не делают! Банки приглашают клиента лично посетить офис для этой цели. Также мошенники могут представляться сотрудниками «полиции» с требованием выкупить родственника попавшего в Камеру Предварительного Заключения.

При таких звонках следует связаться с родственником по телефону, чтобы убедиться, что вы разговаривали с мошенником.

Дропперы.

это люди, которые предоставляют свои банковские карты или счета для проведения незаконных операций. Чаще всего они становятся частью цепочки по выводу или обналичиванию денег, полученных мошенническим путём. Таких людей могут использовать мошенники, с целью избежать их раскрытия и наказания.

Простыми словами, дроппер — это посредник между преступниками и жертвами, который помогает скрыть следы финансовых операций.

Группы риска.

Кибер-аферисты зачастую высоко интеллектуальны, умны и коварны. Они неплохие психологи, тщательно планируют интернет-преступления и прекрасно манипулируют людьми. Существуют определенные группы людей, которые более подверженные риску стать жертвами кибер-мошенничества:

• Пожилые люди: Пожилые люди часто менее знакомы с современными технологиями и интернетом, что делает их уязвимыми к различным уловкам мошенников. Они могут не осознавать риски, связанные с онлайн-операциями, и легко поддаваться манипуляциям. Мошенники могут использовать тактики, такие как создание ложных историй о необходимости помощи или угрозы, чтобы заставить пожилых людей передать свои деньги или личные данные.

• Молодежь: Молодые люди, особенно студенты, могут быть менее осторожными и более доверчивыми, что делает их мишенью для мошенников. Они часто активно используют социальные сети и могут не осознавать, что их личная информация может быть использована против них. Мошенники могут использовать привлекательные предложения, такие как бесплатные подарки или конкурсы, чтобы собрать данные или деньги.

• Пользователи социальных сетей: Люди, активно использующие социальные сети, подвержены риску фишинга и других мошеннических схем. Мошенники могут создавать поддельные аккаунты, выдавая себя за знакомых или знаменитостей, чтобы получить доступ к личной информации. Кроме того, они могут использовать социальные сети для распространения

ложной информации о инвестициях или финансовых возможностях, что может привести к значительным потерям.

• Люди, испытывающие финансовые трудности: Мошенники часто нацеливаются на тех, кто находится в сложной финансовой ситуации, предлагая им "легкие" способы заработка или финансовую помощь. Эти предложения могут выглядеть очень заманчиво, но на самом деле они могут привести к еще большим финансовым потерям. Люди, испытывающие стресс из-за долгов или нехватки денег, могут быть менее осторожными и более склонными к риску.

• Технически неподкованные пользователи: Люди, не обладающие достаточными знаниями о безопасности в интернете, могут легко стать жертвами различных схем. Они могут не знать, как распознать фальшивые сайты, подозрительные электронные письма или вредоносные программы. Мошенники могут использовать сложные методы, такие как подделка адресов сайтов или создание ложных приложений, чтобы обмануть таких пользователей и получить доступ к их личной информации или финансам.

• Люди, находящиеся под стрессом: Мошенники могут воспользоваться эмоциональным состоянием жертв. (3)

• Дети и подростки: Легче поддаются манипуляциям со стороны взрослых. Из-за недостатка финансовой грамотности они не могут отличить предложения подзаработать от противозаконных действий.

Дети при общении с незнакомцами более доверчивы. Они могут поделиться личной информацией не только о себе, но и о своих родственниках, на которых нацелены мошенники.

Последствия кибер-мошенничества.

Финансовые потери: Одним из самых очевидных последствий кибер-мошенничества являются финансовые потери. Жертвы могут потерять значительные суммы денег, что может привести к долговым обязательствам и финансовым трудностям. В некоторых случаях потеря может быть настолько велика, что жертвы вынуждены обращаться за помощью к кредитным учреждениям или социальным службам. Это может также привести к снижению уровня жизни и невозможности удовлетворять базовые потребности, такие как жилье, еда и медицинское обслуживание.

Психологические последствия: Жертвы мошенничества могут испытывать стресс, тревогу и депрессию. Чувство вины и стыда за то, что

они стали жертвами мошенников, может негативно сказаться на их психическом здоровье. Многие жертвы могут испытывать посттравматический стресс, что может привести к социальной изоляции и снижению качества жизни. Они могут также стать более подозрительными и недоверчивыми к окружающим, что затрудняет восстановление нормальных отношений.

Утрата личных данных: Кибер-мошенничество может привести к утечке личной информации, такой как номера кредитных карт, пароли и другие конфиденциальные данные. Это может привести к дальнейшим кражам личных данных и мошенничеству. Утечка данных может также повлечь за собой необходимость долгосрочного мониторинга кредитной истории и постоянного изменения паролей, что создает дополнительные неудобства и стресс для жертвы. В некоторых случаях жертвы могут столкнуться с проблемами, связанными с идентификацией, когда мошенники используют их данные для совершения преступлений

Проблемы с кредитной историей: если мошенники используют личные данные жертвы для получения кредитов или займов, это может негативно сказаться на кредитной истории, что затруднит получение кредитов в будущем. Плохая кредитная история может привести к повышению процентных ставок и отказам в кредитах, что ограничивает финансовые возможности жертвы. Восстановление кредитной истории может занять много времени и потребовать значительных усилий, включая взаимодействие с кредитными бюро и финансовыми учреждениями.

Уголовные последствия: в некоторых случаях жертвы могут стать объектами уголовного преследования, если мошенники используют их личные данные для совершения преступлений.

Это может привести к юридическим проблемам, включая необходимость защиты своих прав в суде и взаимодействия с правоохранительными органами. Жертвы могут столкнуться с обвинениями в мошенничестве или других преступлениях, что может негативно сказаться на их репутации и будущем. Кроме того, процесс разбирательства может быть длительным и эмоционально тяжелым, добавляя к стрессу и тревоге, которые уже испытывает жертва.

Как видим, последствия могут быть поистине разрушающими. Поэтому необходимо уметь противостоять и защищаться от бесконтактного интернет мошенничества.

Рекомендации по безопасному использованию интернета.

На основании полученных результатов я разработал практические рекомендации по безопасному и эффективному использованию интернет:

Будьте осторожны с личной информацией.

• Не делитесь личной информацией, такой как адрес, номер телефона, финансовые данные и пароли, в социальных сетях или на незнакомых веб-сайтах. Мошенники могут использовать эти данные для несанкционированного доступа к вашим аккаунтам или даже для кражи вашей личности.

• Проверяйте настройки конфиденциальности на своих аккаунтах и ограничивайте доступ к личной информации. Убедитесь, что только доверенные лица могут видеть вашу активность и данные. Используйте функции, позволяющие контролировать, кто может видеть вашу информацию.

• Прежде чем предоставлять свои данные, уточните, для каких целей они будут использованы, и проверьте, есть ли у компании политика конфиденциальности. Понимание того, как ваши данные будут обрабатываться, поможет снизить риски.

Осторожно относитесь к электронным письмам и сообщениям.

• Не открывайте вложения и ссылки в подозрительных письмах или сообщениях, особенно от незнакомых отправителей. Мошенники часто используют фишинг, отправляя сообщения с просьбами предоставить личные данные или кликнуть на вредоносные ссылки.

• Проверяйте адреса отправителей на наличие ошибок или подозрительных доменов. Иногда мошенники используют адреса, которые выглядят похожими на настоящие, но содержат небольшие изменения, трудно заметные на первый взгляд.

• Если вы получили сообщение, которое выглядит официально, но сомневаетесь в его подлинности, обратитесь к организации напрямую через официальный сайт или номер телефона, чтобы подтвердить информацию. Не используйте контакты, предоставленные в подозрительном сообщении.

Защищайте свои учетные записи.

Придумывайте сложные уникальные пароли для своих аккаунтов. Чтобы защитить учётную запись от взлома, пароль должен содержать буквы разных регистров, цифры и символы.

Будьте осторожны с сообщениями.

Не отправляйте СМС на короткие номера, не узнав прежде их реальную стоимость! Не оставляйте номер своего мобильного на сомнительных сайтах! (4)

Практическая часть

Для того, чтобы выяснить, достаточно ли информированы ученики школы «МБОУСОШ №15 с. Бада» о финансовой безопасности в интернете, я провел опрос среди 8, 9, 10 и 11 классов. Участие в опросе приняли 84 учащихся. (Приложение 1)

Проанализировав все результаты опроса, можно сделать следующие выводы:

- В опросе приняли 26,2% из 8 классов, 26,2% из 9 классов, 31% из 10 класса и 16,7% из 11 класса.
- Большинство опрошенных учеников (83,3%) используют интернет каждый день.
- Большая часть опрошенных (76,2%) знают, что такое мошенничество в интернете и способы защиты.
- Большую заинтересованность о мошенничестве проявляют 10,11 классов (31%). Но, несмотря на это, остальные так же проявляют интерес.

Вывод: Опрос показал, что ученики знают, какой информацией не следует делиться в интернете и социальных сетях, что нужно осторожнее относиться к незнакомым людям в интернет-пространстве, что ненужно переходить по непроверенным ссылкам и сайтах и тому подобное (Приложение 2).

Мною была проведена беседа с 10А классом, благодаря чему, ученики узнали новые схемы мошенничества и как не попасться на уловки кибер-преступникам (Приложение 3).

Я создал буклет, с информацией о кибермошенничестве и рекомендациями по безопасному использованию сети Интернет с примерами разного вида мошенничества (Приложение 4).

Заключение.

Подводя итоги, можно смело сказать, что кибермошенничество – серьезная угроза, с которой рано или поздно может встретиться каждый. И чтобы этого не произошло, каждый человек должен знать, что это такое и как этого избежать. Повышение осведомленности – главный метод борьбы с мошенничеством.

Задачи, поставленные мною успешно выполнены: я рассмотрел, что такое кибермошенничество, его виды и способы борьбы с ними; я провёл опрос среди 8-11 классов и результаты показали, что ученики довольно хорошо знают, что такое кибермошенничество в целом. Мой проект цели достиг.

Список литературы.

1. https://journal.sovcombank.ru/sberezheniya/chto-takoe-kibermoshennichestvo-i-kak-ot-nego-zaschititsya
2. https://vc.ru/promo/322969-kak-doverie-i-nevnimatelnost-obogatili-moshennikov-na-sotni-milliardov-dollarov-za-50-let
3. https://iz.ru/1843018/2025-02-22/ekspert-nazvala-naibolee-podverzennye-kibermosennicestvu-kategorii-naselenia
4. https://www.kaspersky.ru/resource-center/preemptive-safety/top-10-preemptive-safety-rules-and-what-not-to-do-online.
5. Левитан, А. (2020). "Интернет и образование: возможности и риски". Журнал педагогических исследований

Приложение

Приложение 1

Опрос:

1. В каком классе вы учитесь?

2. Как часто ты используешь интернет?

3. Знаешь ли ты, что такое мошенничество в интернете и как защитить себя в интернет сетях?

4. Какие из следующих угроз ты знаешь?

5.Как ты защищаешь свои личные данные в интернете?

6. Как ты относишься к незнакомым людям в интернете?

7. Используешь ли ты функции безопасности в социальных сетях?

8. Получал(а) ли ты когда-нибудь подозрительные сообщения или письма в интернете?

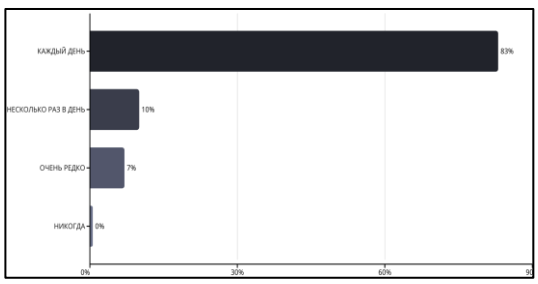
9. Какие действия ты бы предпринял(а), если бы получил(а) подозрительное сообщение в интернете?

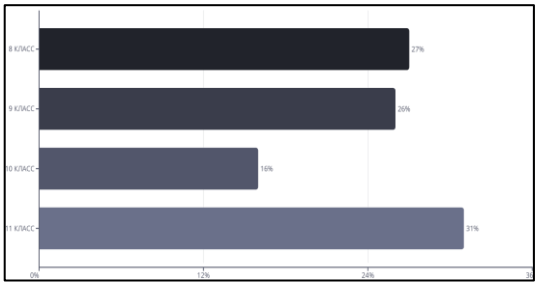
10. Какой информацией, по твоему мнению, не следует делиться в интернете?

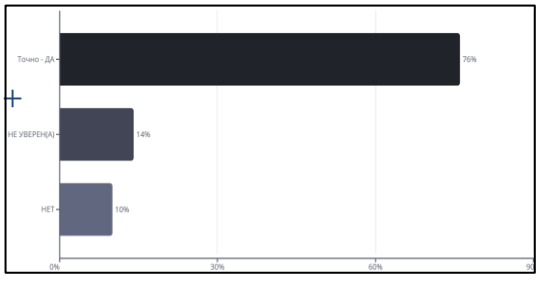
11. Какие советы по безопасности в интернете ты можешь дать своим друзьям?

Приложение 2

Результаты опроса







Приложение 3

Приложение 4