ПРОЕКТ:

ПРАВОВОЕ

ПРОСВЕЩЕНИЕ

НА ЮФ ВСГУТУ

Тема:

Информационная безопасность

Улан-Удэ
2021

Положительные и отрицательные стороны ИНТЕРНЕТА

Положительные стороны	Отрицательные стороны
Общение с друзьями/семьей	Компьютерный «вирус»
Доступ к информации и развлечениям	Злоумышленники могут взломать адрес учетных записей
Учиться знакомиться с новыми людьми и узнавать новое	Хакеры могут отправлять смс, которые взламывают пароли от банковских карт
Помощь в учебе	Увеличились махинации с финансовыми пирамидами
Возможность найти психологическую поддержку	Общение может негативно влиять

Законодатель нашей страны понимает опасность в которой себе таит ИНТЕРНЕТ для детей и подростков, поэтому был издан Федеральный закон от 29 декабря 2010 г. № 436 «О защите детей от информации, причиняющей вред их здоровью и развитию»

Возраст, с которого ты можешь получить банковскую карту

От 6 до 14 лет, дополнительная карта, открытая к карте на родителя

С 14 до 15 лет в виде основной карты при согласии родителя

С 16 лет законодательство позволяет уже открывать платежную карту САМОСТОЯТЕЛЬНО

Мошенничество в сети

Мошенничество в сети может осуществляться в достаточно большом количестве способов, но все их перечислить очень сложно, поэтому мы с тобой рассмотрим некоторые наиболее распространенные.

«Опасный заработок»

Ты скорее всего, сталкивался с трудностями в деньгах, например, когда хотел себе купить модную одежду/гаджет, пойти в кинотеатр/кафе и прочее.

ЗАПОМНИ! Мошенники пользуются этим и могут убедить тебя «быстро заработать» и попросить вложить деньги в «сверхприбыльный проект» – это называется финансовая пирамида. От нее нельзя получить прибыль, а только убытки.

Суть и реальные примеры финансовых пирамид

Суть финансовой пирамиды проста: приноси свои деньги сегодня, а завтра забирай их с прибылью.

Популярная финансовая пирамида Улан-Удэ «ФИНИКО»

Главным вдохновителем российских финансовых пирамид можно назвать Сергея Мавроди и его компанию «МММ». Фирма выпустила 991 000 акций, которые продавала за тысячу рублей.

«Букмекерские ставки»

Мошенники могут тебе предложить просто зарегистрироваться на сайте, чтобы за реальные деньги ты смог поставить ставку на различных играх. Для того, чтобы забрать свой выигрыш они «якобы» просят заплатить комиссию через банковскую карту. Итог: данные карты и деньги остаются у них.

Обман мошенников о помощи от имени друзей в соц. сетях

Киберпреступник может взломать аккаунт в соц. сетях, а затем от чужого имени написать сообщение по списку друзей.

Запомни, если тебе пришла подозрительная смс, где тебя просят: «одолжи деньги в долг», «дай в займы» и т.д. не ленись и лучше позвони и спроси, действительно ли, нужна помощь или задай вопрос, который застанет преступника врасплох.

Еще одна уловка может быть со ссылками, где вместо фотографии присылают вредоносный вирус. Он крадет с гаджета персональные данные, логины и пароли от личных кабинетов, в том числе от банковских.

Защититься от вредоносных ссылок помогут антивирусы, которые можно установить на всех гаджетах.

ПРАВИЛА БЕЗОПАСНОСТИ В СЕТИ

- ✓ **Будь аккуратным со ссылками, содержащимися в электронных письмах и личных сообщениях;**
- ✓ **Не отправляй конфиденциальную, личную или финансовую информацию;**
- ✓ **Будь внимателен! Фальшивые, похожие на сайты крупных компаний веб-сайты предназначены для обмана клиентов для сбора их личной информации;**
- ✓ **Не совершай покупки в Интернете, не обсудив это с родителями;**
- ✓ **Не общайся с незнакомцами в Сети и не переходи по подозрительным ссылкам;**
- ✓ **Если кто-то из твоих друзей внезапно попросит перечислить ему деньги, обязательно перезвони этому человеку и узнай, действительно ли, ему нужны деньги.**

Борьба с мошенничеством в ИНТЕРНЕТЕ

Напиши вместе с родителями заявление в отдел по защите прав потребителей.

К такому документу приложи все имеющиеся чеки.

Не забудь написать жалобу и в полицию по факту мошенничества!!!

Уголовный Кодекс предусматривает уголовную ответственность за мошенничество в компьютерной информации (ст. 159.6 УК РФ).

Кибербуллинг или виртуальное издевательство

Кибербуллинг — это преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

ПОСЛЕДСТВИЯ КИБЕРБУЛЛИНГА

58%

взрослых были вынуждены вмешаться, *чтобы помочь ребенку*

13%

виртуальных конфликтов *переросли в реальные*

7%

пострадавших получили ***настолько тяжелую психологическую травму,*** *что длительное время переживали случившееся*

26%

родителей ***узнали об инцидентах кибербуллинга намного позже*** *того, как они случились*

---

*Исследование проведено аналитическим агентством B2B International специально для «Лаборатории Касперского» летом 2014 года. В ходе исследования было опрошено 11135 респондентов – домашних пользователей в возрасте 16+, проживающих в странах Латинской и Северной Америки, Ближнего Востока, Азии, Африки, Европы и России в частности.

Основные советы по борьбе с кибербуллингом

1. **Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;**
2. **Управляй своей киберрепутацией;**
3. **Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;**
4. **Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно. ПОМНИ ДАЖЕ УДАЛЕННЫЙ ТЕКСТ МОЖНО ВОССТАНОВИТЬ, а этим уже занимаются специальные службы;**
5. **Веди себя вежливо;**
6. **Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;**
7. **Бань агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов.**

Шанс попасть в руки педофила

Жертвами виртуальных педофилов в последние годы все чаще становятся дети. Безобидная переписка в интернете перетекает в недвусмысленные намеки и обмен фотографиями интимного характера.

Сегодня интернетом активно пользуются 72% российских подростков. Каждый второй ребенок, зарегистрированный «ВКонтакте», хотя бы раз получал сообщения интимного характера.

Отдельная тема, которая становится все актуальнее, – интернет-груминг, когда взрослый устанавливает дружеский контакт с ребенком через соцсети, чтобы затем в реальной жизни склонить его к сексуальному контакту.

Что нужно делать, чтобы не попасть в руки педофила?

Не публикуй в интернете свою личную информацию – ФИО, ФИО родителей, адрес, номер телефона, номер школы

Не общайся с незнакомцами в сети

Не верь информации, которую тебе сообщает незнакомец. Фото, имя, и прочие сведения зачастую могут быть ложными.

Не обменивайся фотографиями с незнакомцами

Не соглашайся на встречи с незнакомцем из интернета. Если ты все же пойдешь на встречу, обязательно обсудите это с родителями

Обязательно сообщай родителям, если ты столкнулся в Интернете с педофилом. Они также могут обратиться в полицию: в РФ предусмотрено наказание за действия сексуального характера с детьми статьей 134 УК РФ.

Шантаж

Распространены случая шантажа в сети, когда просят заплатить выкуп в обмен на нераспространение компрометирующей информации.

Попав в такую ситуацию, не поддавайся на уловки злоумышленников и не переводи деньги, потому, что:

- **подобные угрозы зачастую безосновательны. К тому же, полной уверенности в том, что вымогательство не повторится снова, у тебя никогда не будет;**
- **не выходи с шантажистом на связь;**
- **обратись с родителями в полицию по месту вашего жительства с заявлением о вымогательстве, приложив скриншоты сообщений;**
- **сообщи полиции номер телефона, на который мошенники просят перевести деньги, и суть мошенничества;**
- **чтобы минимизировать такие риски в будущем, сделай профиль «закрытым», внимательно относись к новым знакомствам, периодически меняй пароли, подбирая сложные комбинации.**

Ответственность за шантаж

Преступника за шантаж можно привлечь к уголовной ответственности по статьям

163 УК РФ «Вымогательство»

Максимальное наказание лишение свободы на срок до семи лет

137 УК РФ «Нарушение неприкосновенности частной жизни»

предполагает лишение свободы на срок до двух лет

Возраст, ответственности наступает с 16 лет

ПРАВИЛА БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ

№1. ХРАНИ ТАЙНЫ

В информационном пространстве нам часто приходится вводить свои данные: ФИО, адрес, дату рождения, номера документов. **Безопасно ли это?**

Персональные данные (имя, фамилия, адрес, дата рождения, номера документов) можно вводить в том случае, если соединение устанавливается по протоколу **https**. Слева от адреса сайта должен появиться значок в виде зеленого замка — это означает, что соединение защищено.

Важно помнить, что ни в коем случае нельзя передавать через Сеть данные любых документов и банковских карт. Даже (и тем более) если кто-то об этом просит, старается убедить в том, что возникла критическая ситуация, торопит и повторяет, что нужно срочно прислать информацию.

№ 2. БУДЬ АНОНИМНЫМ

Создавая свой профиль в социальных сетях, нужно максимально избегать привязки к «физическому» миру.

Нельзя указывать свой адрес, дату рождения, школу, класс. Лучше использовать очевидный псевдоним: по нему должно быть ясно, что это не настоящее имя (ведь использовать ложные данные: «Алексей» вместо «Александр» — по правилам соц. сетей запрещено).

Не надо ставить свою фотографию на аватар, если тебе не исполнилось хотя бы 15-16 лет. Все дети и подростки младше этого возраста, публикуя свою фотографию, рискуют стать жертвой злоумышленника.

№ 3. Не сообщайте свое местоположение

Данные геолокации позволяют всему миру узнать, где ты живешь и учишься, проводишь свободное время, какие шоу и спектакли любишь, как отдыхаешь. Отследить местоположение человека теперь не составляет труда.

Для тебя это может представлять большую опасность. Чтобы сделать геолокацию максимально безопасной, нужно следить за тем, чтобы местоположение не отображалось на «искабельных» объектах — особенно на фотографиях. На телефонах, в настройках камеры, как правило, можно запретить геометки.

№ 4. НАУЧИСЬ ЗАМЕЧАТЬ ПОДДЕЛЬНЫЕ САЙТЫ

Фишинг — это способ выманивать у человека его данные: логин, название учетной записи и пароль.

Происходит это так: пользователю присылают ссылку на сайт, очень похожую на настоящий адрес почтового сервиса или социальной сети. Как правило, фишеры специально покупают такие домены. Например, для mail.ru это может быть «meil.ru», а для vk.com — «vk-com.com».

Злоумышленник ждет, когда человек введет логин или пароль на поддельном сайте. Так он узнает данные, а потом использует их для входа в настоящий профиль своей жертвы.

№ 5. АККУРАТНЕЕ С ПОКУПКАМИ

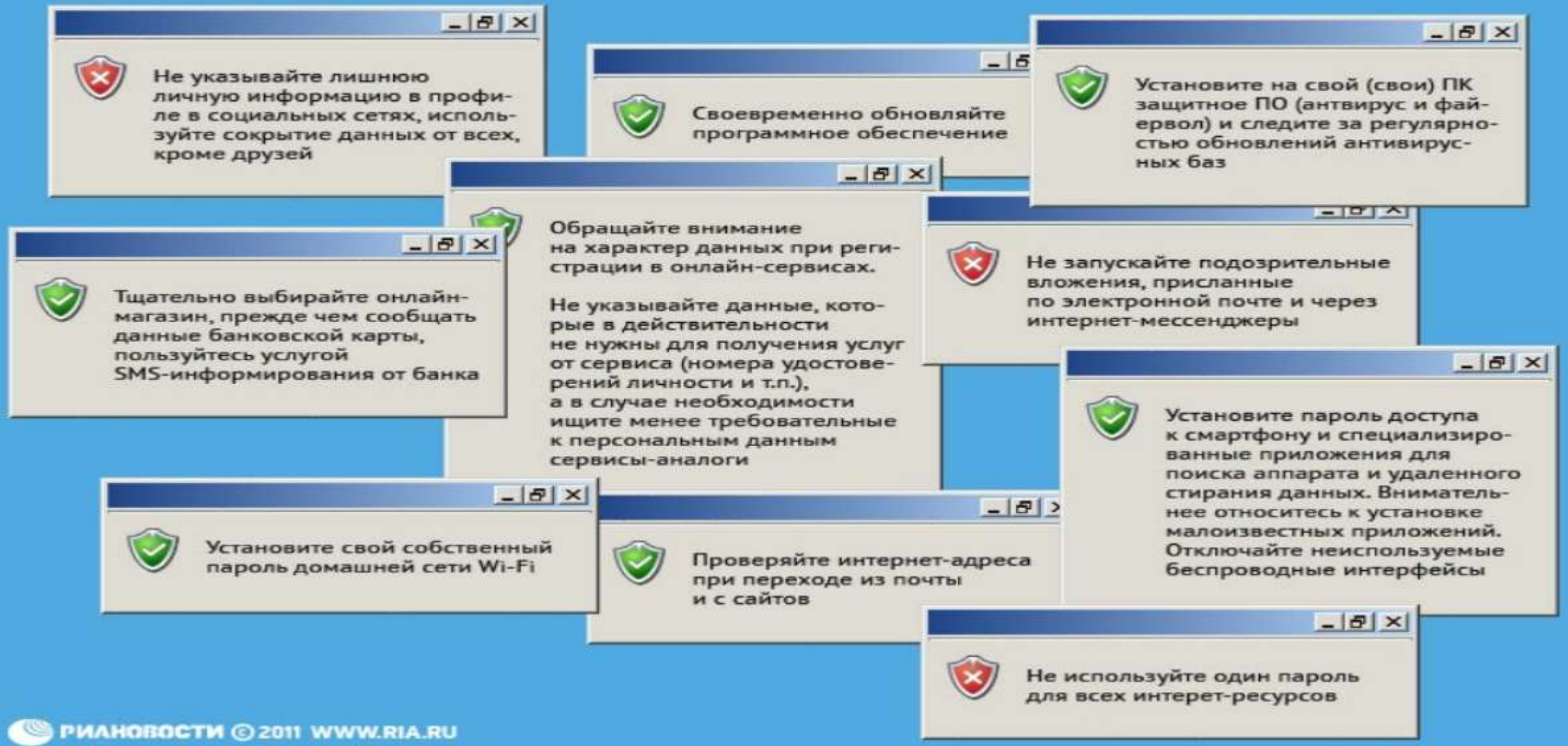
Основные финансовые потери обычно происходят через телефон. Необходимо подключить услуги блокировки платного контента, не класть много денег на счет телефона и контролировать расходы. Все остальные платежи должны согласовываться с родителями и происходить только под их присмотром.

Все сервисы, которые принимают деньги, должны иметь зеленый значок «https» рядом с названием. Если такого значка нет, лучше не пользоваться страницей. Впрочем, даже его наличие стопроцентной гарантии не дает.

Часто в пабликах «ВКонтакте» предлагают что-то купить с использованием платежной системы Qiwi. Тут тоже нужно проявлять бдительность и внимательно изучать отзывы о продавце. В соцсетях есть немало мошенников, которые после получения денег исчезают.

10 способов защиты личных данных

Как не стать жертвой интернет-мошенников



Презентация подготовлена в рамках работы Центра правового просвещения и профессиональной адаптации студентов ВСГУТУ.

Руководитель Центра: д.ю.н., доцент Е.И. Попова.

Материал подготовлен по состоянию на 01.12.2021 г.

СПАСИБО ЗА ВНИМАНИЕ!

Авторы-составители:

Студенты ВСГУТУ юридического факультета
Первая Кристина Олеговна
Меньжурова Елена Александровна
Иванова Анна Алексеевна