**ТЕХНОЛОГИЧЕСКАЯ КАРТА ЗАНЯТИЯ**

|  |  |
| --- | --- |
| **Тема**  | «Осторожно! Мошенничество в сети» |
| **Класс**  | 10-11 класс и студенты |
| **Форма занятия** | Видеолекция с элементами беседы и практикума  |
| **Цель урока**  | Формирование у учащихся навыков безопасности при работе в сети |
| **Планируемые результаты** | **Предметные:**Формирование представления:- о финансовом кибермошенничестве в сети, его видах и первоочередных шагах для обеспечения безопасности.Формирование знаний:- об эволюции денег и их классификации;- о том, как меняется финансовый мир вокруг нас и наше поведение при переходе от информационной эры к цифровой;- о видах финансового кибермошенничества и правилах безопасности в сети.**Метапредметные**:- уметь оперировать финансовыми понятиями, изученными на уроке: -различные виды денег: что общего и чем отличаются;-электронная платёжная система и электронный кошелёк;-бесконтактные платежи; -фишинг; кибермошенничество; SCAM; маркетплейс; овердрафт; VPN-новые технологии: боты и чат-боты.**Личностные:**Формирование понимания, что:- в ближайшие 10 лет технологии радикально изменят наш мир;- азы цифрового поведения необходимы для жизни в новом цифровом мире;- технологии облегчат нашу жизнь, но вместе с тем и возможностей стать жертвой финансового мошенничества тоже станет больше;- чтобы не стать жертвой финансовых кибермошенников, нужно обладать навыками безопасности при пользовании гаджетами и приложениями. |
| **Оборудование** | Проектор, экран |
| **Расстановка парт и стульев** | Любая |
| **Расходный материал** | Листы формата А4, карандаши |
| **Дидактический материал** | Видеозапись лекции, раздаточный материал (задачи) |

**ТАЙМИНГ ЗАНЯТИЯ**

|  |  |  |
| --- | --- | --- |
| **ЭТАП 1. Введение; несколько вопросов для введения в тему** | Слайд №1 | 1- 2 мин. |
| **ЭТАП 2. Основная часть**1. **Эволюция денег**
 | Слайды №2-8 | 12-14 мин. |
| 1.Что такое мошенничество и кибермошенничество. Первая финансовая пирамида в России | Слайд №2 | 2 мин. |
| 2.Виды денег и их эволюция | Слайды №3-4 | 3 мин. |
| 3.Как происходят безналичные и электронные расчеты. Что такое электронные деньги. Интересная статистика | Слайды №5-6 | 5 мин. |
| 4. Криптовалюта (криптоденьги) | Слайд №7 | 2 мин. |
| 5. Игровая валюта и валюта корпоративного значения | Слайд №8 | 2 мин. |
| 1. **Мошенничество в сети**
 | Слайды № | 25-28 мин. |
| 1.ЭПС и электронный кошелек | Слайд №9 | 3 мин. |
| 2.Банковская карта. Кошелек в смартфоне | Слайды №10-12 | 4 мин. |
| 3.Покупки товаров сети. Маркетплейсы | Слайды №114 | 2-3мин. |
| 4.Мошенничество в соцсетях:ВконтактеИнстаграмTik Tok | Слайд№15-18Слайд №15-16Слайд№17-18Слайд №19 | 10-12 мин |
| 5. Мошенничество в YouTube | Слайды №20 | 2 мин. |
| 6.Мошенничество в мессенджере Telegram | Слайд №21-23 | 4 мин |
| **ЭТАП 3. Подведение итогов** | Слайды №24-27 | 15 мин. |
| 1.Советы | Слайд №24 | 1 мин. |
| 2.Вопросы | Слайд №25 | 3 мин. |
| 3.Решение задач. Выполнение заданий | Слайды№26-27 | 10 мин. |

**Рекомендации по проведению занятия**

**Введение**. (Несколько слов о Неделе финансовой грамотности для детей и молодежи).

Перед началом занятия, буквально на 1-2 минуты, необходимо настроить учащихся на работу, пробудить у них интерес к теме.

*- Сегодня нас с вами ждет встреча с миром цифровых технологий. Мы разберемся в устройстве современных финансовых услуг; поговорим про виды кибермошенничеств и угроз, которые исходят из сети; узнаем, как можно обнаружить эти угрозы и избежать.*

**Можно задать вопросы:**

*-Поднимите руку, у кого есть смартфон? Вы заходите со своего смартфона в соцсети?*

*-А кто установил приложение и расплачивается в магазинах телефоном вместо карты?*

Для молодых людей поколения Z, двери в финансовый рынок открываются не через офисы банков, а через мобильные устройства.

Поэтому крайне важно научиться грамотному цифровому поведению, навыкам безопасности при пользовании гаджетами и приложениями, чтобы уметь противостоять мошенникам, количество которых растет каждый год.

**ОСНОВНАЯ ЧАСТЬ**

**ПЕРВАЯ ЧАСТЬ. Эволюция денег и их классификация**

Сейчас уже сложно представить свою жизнь без банковских карт и оплаты покупок через интернет. Будущее уже наступило. Но и финансовые мошенники не дремлют.

Давайте поговорим про эволюцию денег и виды финансового мошенничества и финансового кибермошенничества.

1. **Кибермошенничество**

***Слайд №2***

В основе мошенничества лежит обман, который был известен еще законодателям Древнего Рима.

*Мошенничество — хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием.*

**Интересные факты**

Известия о мошенниках стали появляться в царской России в 17 веке.

**Первая финансовая пирамида в России**

*Автор первой финансовой пирамиды стал руководитель общественного банка города Скопин Рязанской губернии Иван Рыков еще в XIX веке. Молодой человек предлагал горожанам вклады под очень высокий процент — 7,5. В то время как другие банки давали максимум 3 процента.*

*Рыков уже в то время знал, как убедить людей: публиковал липовые отчеты; выдал обещанную прибыль первым вкладчикам. И как следствие в банк сразу же выстроилась очередь. В сеть к проходимцу попались многие богатые купцы и ремесленники. Его афера длилась почти 15 лет, а потом во время ревизии выяснилось, что касса, в которой числилось 13 миллионов рублей пуста…*

Современные технологии значительно облегчили нашу жизнь, но вместе с тем появилась реальная угроза стать жертвой финансовых кибермошенников. Это слово звучит странно, напоминая футуристические научно-фантастические романы. Но будущее уже наступило.

*Финансовое кибермошенничество - это преступная деятельность, целью которой является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, пароли и т.д.)*

Большинство кибермошенничеств совершаются киберпреступниками или хакерами, которые зарабатывают на этом деньги.

**Примеры киберпреступлений:**

1. Мошенничество с электронной почтой
2. Кража данных банковских карт
3. Мошенничество в соцстетях
4. Атаки вирусных программ

И во время нашего урока сегодня мы с вами будем рассматривать все возможные способы защиты ваших персональных данных в сети, и, соответственно, ваших денег. Давайте сначала поговорим с вами, что такое деньги и откуда они берут свое начало.

1. **Виды денег и их эволюция**

***Слайд №3***

**Вопрос:**

*- Что такое деньги?*

*- Откуда они берут свое начало? Давайте разбираться.*

**Де́ньги** — эквивалент, служащий мерой стоимости любых товаров и услуг, способный непосредственно на них обмениваться.

*По преданию, богиня Юнона во время войны с Пирром ответила римлянам, что у них не будет недостатка в деньгах, если они будут справедливо вести войну. Когда это обещание сбылось, римляне назвали ее Монетой (анг. Moneta – советница, наставница) и стали изображать на отчеканенных деньгах в 269 до н.э. От Монеты произошли современные слова «монетный двор» и англ. money (деньги).*

**Выделяют 4 основных этапа эволюции денег**

***1 этап – обмен на товары (бартер), прообраз денег (ракушки, шкуры и т.д.)***

Бартер на Руси проходил те же этапы в своем развитии, что и в других странах. В северных областях «товарными» деньгами служили шкурки куниц, белок, лисиц.

***Интересные факты:***

*Самый знаменитый пример бартера - сделка Питера Миноты в 1626 году: за бусины и безделушки, стоимостью 24$ Минота получил остров в Манхеттене. По расчетам американских финансистов стоимость земли острова Манхэттен оценивается в сумму порядка 49 миллиардов долларов.*

***2 этап – металлические деньги. Первая монета – прообраз современной, появилась в 7 веке до*** н.э., в Лидии (территория Турции). На Руси монеты появились в Х века, они чеканились из серебра.

***3 этап - закрепление за золотом роли всеобщего стоимостного эквивалента***

***4 этап – появление современных денег***

Его можно разделить на три основных момента:

*4.1.переход к бумажным деньгам. Банкир выдавал клиенту расписку (квитанцию) о внесении ценностей в свой банк. В другом городе, клиент предъявлял эту расписку в банке и мог получить свои ценности золотом или монетами.*

*4.2. постепенное вытеснение наличных денег из оборота. Появляются безналичные деньги в виде записей на банковских счетах, чеки, векселя, ценные бумаги (акции и облигации); и банковская карта.*

*4.3. появляются электронные/цифровые деньги*

**Давайте рассмотрим современные виды денег, представленные в таблице.**

**Виды денег**

***Слайд №4* См. таблицу**

1. **Как происходят безналичные и электронные расчеты**

***Слайд №5***

**Безналичные расчеты** - Это платежи без использования наличных денег путем перечисления денежных средств по счетам в кредитных организациях и зачетов взаимных требований.

Отличительный признак данного вида расчетов – наличие счета в банке. Счет – это запись остатков в результате движения денежных средств.

**Примеры**

1. Вы оплатили год подписки на музыку в сумме 1000 рублей и перечислили со своего счета в банке Стандарт на счет ООО «Музыка» в банке Магнит. Такая операция признается безналичным расчетом.
2. Если вы перевели 500 рублей за билеты в театр своему другу, то у вас по счету будет сделана запись: минус 500 рублей. А по счету вашего друга будет сделана запись о приходе данной суммы.
3. Вы получили зарплату и положили себе на карту 10 000 рублей, то по вашему счету в банке будет произведена запись «+10 000 рублей».

 **- А что делать, если банковский счет не открыт? Как перевести деньги?**

В этом случае мы используем субсчета в организациях:

* банка, где операционист проводит оплату вашей квитанции ЖКХ
* ЭПС (электронной платежной системы), где вы открыли электронный кошелек
* системы денежных переводов, через которые вы отправляете деньги и т.д.

**Электронные деньги**

***Слайд №6***

**Вопрос:**

*- Как вы считаете, когда появилась электронная валюта?*

Ответ: В 1918 году в в США бы осуществлен первый в истории безналичный платеж при помощи телеграфа.

**Вопрос:**

*- Ребята, что для вас удобнее: пользоваться наличными деньгами или электронными?*

**Интересная статистика**

*Национальных агентством финансовых исследований (НАФИ) в 2019 году был проведен опрос населения и вот что выяснилось. Среди опрошенных:*

* 19% не посещают офис банка. Решают все вопросы удаленно (онлайн)
* 31% посещают офис реже одного раза в месяц
* 67% используют интернет и мобильный банк
* 11% используют бесконтактную карту
* 3% используют умные часы и браслеты

**Что такое электронные деньги?**

Электронные деньги - это виртуальные денежные единицы, посредством которых осуществляются всевозможные расчеты в сети интернет. Это, по сути, те же денежные знаки, имеющие такую же ценность, как и реальные деньги или средства на банковских счетах, с той разницей, что весь их оборот происходит исключительно в интернете. Электронные деньги могут быть в разных валютах, их можно обменять на реальные деньги и наоборот.

**Вопрос:**

*Чем электронные деньги отличаются от безналичных?*

Безналичные деньги находятся в банке на расчетном или текущем счете и вы ими можете управлять, например, с помощью банковской карты.

Электронные деньги находятся в кредитной организации, которая имеет право переводить средства без открытия банковских счетов. Эта организация выступает в роли ОПЕРАТОРА электронных денежных средств. Место, где находятся электронные деньги называют ЭЛЕКТРОННЫМ КОШЕЛЬКОМ.

**Электронный кошелек** – это сервис виртуальной (электронной) платежной системы, в котором проводятся расчетные операции. На его счете содержатся деньги, но только представленные не в привычном бумажном выражении, а электронном. Пользователь может распоряжаться ими по своему усмотрению, переводить другим людям, оплачивать услуги или интернет-покупки, выводить на банковские карты.

**Электронная платёжная система** — это система расчётов между финансовыми организациями, бизнес-организациями и интернет-пользователями при покупке-продаже товаров и за различные услуги через Интернет.

1. **Криптовалюта**

***Слайд №7***

Криптовалюта— это новый вид платёжного средства, предназначенный для использования в интернете. Криптовалюта не имеет физических носителей и существует только в виде программного кода. Поэтому её еще часто называют виртуальной или цифровой валютой.

Самой популярной криптовалютой является биткоин.

*Интересные факты*

*1. С момента создания биткоина в 2009 году было несколько предположений о том, кто мог быть основателем биткоина. Сатоши Накомото — псевдоним человека или группы людей, которые создали биткоин. В настоящее время личность создателя самой популярной в мире криптовалюты остается неизвестной.*

*2. Первая транзакция биткоина была произведена для покупки пиццы 22 мая 2010 г. Эта транзакция стала поистине историческим событием, так как с ее помощью купили две самые дорогие пиццы в мире. Программист из штата Флорида Ласло Ханич, решил заказал 2 пиццы за 10 тыс. BTC. На момент транзакции эта сумма соответствовала примерно 41 доллару, в то время как сегодня такое количество биткоинов стоит не менее $ 6,6 млн.*

*3. Монеты появляются в результате процесса, названного как «Майнинг». За 5 лет цена биткоина выросла с 0 до около 16 тыс. долларов США. Миллион биткоинов был взят лично Сатоси и по всей видимости до сих пор ему принадлежит. В 2140 году будет добыт последний биткоин. 21 млн. — максимальное количество биткоинов, которое можно добыть.*

**Мошенническая схема с с криптовалютами**

Махинации с криптовалютами – один из самых популярных видов киберпреступлений. Например, сбор средств на развитие проектов в сфере криптовалют. Мошенники могут продавать фальшивую криптовалюту за биткоин или эфириум, которые имеют реальную стоимость. После нескольких раундов сбора средств «новаторы» пропадали без вести вместе с собранными средствами

**Как защититься?**

Для начала изучите рынок криптовалют более детально, прежде чем вкладывать реальные деньги.

1. **Другие виды валют**

***Слайд №8***

**Игровая валюта** (игровое оружие, техника, артефакты, игровые монеты и др.). С правовой точки зрения игровая валюта не может рассматриваться в качестве денег. Это не государственная валюта и предназначена только для целей данной игры.

***Вопрос***

*- Какие вы знаете игровые валюты, назовите?*

**Валюта корпоративного значения** – вознаграждение клиентов за лояльность к компании.

Что это может быть? Бонусы или баллы за каждую покупку; возврат части стоимости за покупку (кешбэк); накопленные мили, которые могут быть потрачены на приобретение билета и т.д. Также не может признаваться деньгами. Введение валюты корпоративного значения связано с маркетинговой политикой компаний.

*Например, вы идете в сетевой магазин, у вас есть карта этого магазина и при покупке товаров вам начисляются бонусы (баллы), которые вы можете использовать при следующей покупке, а иногда и при покупке в магазинах-партнерах.*

***Вопрос:***

 *- Вы пользуетесь бонусами и кешбэком? Назовите сетевые магазины, где можно получить кешбэк за покупку.*

**ЗАДАНИЕ. Придумайте свою платежную систему и свои деньги. Как вы их назовете? Будет ли начисляться кешбэк за покупки? Если да, то какой процент?**

**Вторая часть. БЕЗОПАСНОСТЬ В СЕТИ**

1. **Электронные платежные системы**

***Слайд №9***

***Вопрос:***

*- Как вы думаете, в каком году в России был проведен первый расчет виртуальной валютой?*

**Ответ: В 1998 году.**

В этом же году начала работать платежная система WebMoney. Свой логотип «Муравья» и прозвище «муравейник» система получила благодаря умелой организации расчетов между клиентами называющейся «person to person».

**- Какие еще вы знаете электронные платежные системы?**

**Вот список самых популярных в России ЭПЛ:**

* PayPal. Многие биржи фриланса не сотрудничают с PayPal
* Яндекс.Деньги. Платежная платформа была разработана в 2002 году компанией Яндекс
* Webmoney Один из крупнейших платежных сервисов
* QIWI. Привязка интернет-кошелька в этой системе происходит по номеру мобильного телефона.

**Как завести электронный кошелек**

* Выбрать платежную систему
* Пройти в ней несложную регистрацию
* Подтвердить свою личность

По российскому законодательству без подтверждения личности можно проводить финансовые операции и держать на счете только до 15 тысяч рублей.

**ПРАВИЛА ТЕХНИКИ БЕЗОПАСНОСТИ**

Электронные платежные системы имеют очень высокие уровни защиты. Однако при регистрации кошелька специалисты рекомендуют придерживаться правил безопасности.

См. презентацию

1. **Банковская карта**

***Слайд №10***

Один из самых распространенных способов оплаты сегодня – оплата банковской картой.

**Вопросы:**

 *- Вы знаете, как выглядит банковская карта? Какие должны быть в ней элементы?*

*- Ребята, какие виды банковских карт вы можете назвать?*

Ответ: кредитная, дебетовая, зарплатная, пенсионная, социальная карта.

**КАК ПРЕВРАТИТЬ НАЛИЧНЫЕ ДЕНЬГИ В ЭЛЕКТРОННЫЕ?**

***Слайд №11***

**Для этого нужно**

1. Завести электронное средство платежа. Что это значит? Открыть электронный кошелек или банковскую карту. Что такое электронный кошелек и как его открыть мы с вами уже обсудили.
2. Пополнить электронное средство платежа.

**Вопрос**

*- Как можно пополнить электронный кошелек или банковскую карту?*

А) Внести наличные денежные средства через банкомат или платежный терминал. В этом случае наличные деньги превращаются в электронные.

В) Перевести необходимую сумму с вашего счета на банковскую карту или электронный кошелек. В этом случае безналичные деньги превращаются в деньги электронные.

**КОШЕЛЕК В СМАРТФОНЕ. Бесконтактные платежи**

**Вопрос**

*- У кого к телефону привязана банковская карта?*

Благодаря технологии NFC пользователи могут расплачиваться телефоном, часами или браслетом, в который встроен чип.

Посмотрите на свою банковскую карту, чтобы определить, если на ней возможность бесконтактной оплаты. На банковской карте должен быть отображен значок радиоволн, а также бывает надпись: «PayWave» или «PayPass».

Прежде чем привязать карту к мобильному устройству узнайте, оснащен ли ваш смартфон функцией NFC.

Прежде чем начать пользоваться телефоном, как дебетовой картой, нужно установить специализированное приложение в зависимости от вашего смартфона:

* Эппл Пэй;
* Андроид Пэй;
* Самсунг Пэй.

**Мобильные зловреды**

Наши телефоны знают о нас практически все. И этой информацией очень хотят завладеть киберпреступники.

Шпионские программы могут похищать самые разные данные — от логинов и паролей до фото и геолокационной информации, записывать звук, снимать видео, а также самостоятельно подключаться к wi-fi, чтобы передать всю собранную информацию.

Троян Faketoken, скачанный вместе с разными приложениями, мог перехватить SMS от банка и передать его своим хозяевам, чтобы они могли совершать операции от вашего имени со своего устройства.

**ПРАВИЛА ТЕХНИКИ БЕЗОПАСНОСТИ ПРИ ОПЛАТЕ КАРТОЙ В ИНТЕРНЕТ**

См. презентацию

***Овердрафт*** *– форма краткосрочного кредита, предоставление которого осуществляется путем списания банком средств по счету клиента сверх остатка на его счете.*

**VPN расшифровывается как Virtual Private Network**. В переводе на русский – виртуальная частная сеть. ВПН – это технология, которая обеспечивает зашифрованное соединение поверх вашего интернет-соединения.

***Пример мошенничества «Фейковое СМС от банка»***

*Марине прислали смс с текстом, что ее карта заблокирована (часто сразу звонят на номер телефона). В конце смс был указан номер телефона, по которому нужно связаться с якобы сотрудником банка. Марина позвонила по номеру и попала в руки искусного мошенника, передала конфиденциальные данные и в результате с ее карты было списано 24 000 рублей.*

Как защитится: **никогда и никому не сообщайте свои данные, а также любую банковскую информацию.**

1. **Покупки товаров в сети. Как не нарваться на кибермошенников**

***Слайд №13***

***Вопрос***

*-Вы покупали что-нибудь через интернет? Как вы проверяли надежность продавца?*

Часто нами движет желание сэкономить, чем пользуются мошенники в сети. Они размещают товары на сайтах по очень выгодным ценам- на 30-40% ниже, чем по рынку. Причем часто главное условие покупки: вы должны внести небольшой аванс на карту. После чего и объявление и «продавец» исчезают.

**Как защититься?** См. презентацию

***Маркетплейс*** *- это электронная торговая площадка c большим количеством продавцов. По сути, это сайт-рынок, где встречаются покупатель и продавец, знакомятся, общаются и заключают сделки.*

Все продавцы на маркетплейсах проверены, а цены в большинстве случаев весьма привлекательны. Тем более сейчас почти все известные маркетплейсы предлагают хорошие бонусы и скидки за первую покупку.

**Вопрос:**

*- Ребята, поднимите руки, кто покупал товары в маркетплейсе? В каком?*

**Что делать, если стали жертвой интернет-мошенников?**

***Слайд №14***

Проще предотвратить подобную ситуацию, чем разгребать последствия.

Но если все же вы стали жертвой интернет мошенников, то выполните следующее:

См. презентацию

**Когда будете писать заявление, укажите все данные на мошенников, которые у вас есть:**

* адрес мошеннического сайта;
* ник злоумышленника на форуме;
* номер счета или электронного кошелька, на который были переведены денежные средства;
* номер телефона, на который было отправлено СМС-сообщение;
* адрес электронной почты мошенника и т. д.
1. **Мошенничество в соцсетях**

***Вопрос:***

*- Ребята, какие вы знаете популярные соцсети?*

***Ответ: Вконтакте, Одноклассники, фейсбук, инстаграм, ТикТок***

Давайте разберем, какие есть виды мошенничества в соцсетях и как вы можете защитить свои данные и деньги от киберпреступников.

**Мошенничество во Вконтакте**

***Слайд №15-16***

***Вопрос***

*- Ребята, у кого есть страница во Вконтакте?*

Эта соцсеть очень популярна у мошенников. Давайте разберем с вами основные виды мошенничества во Вконтакте и как их избежать.

1. **Мнимые друзья**

*- Писал ли вам когда-нибудь якобы ваш «друг». Что у него что-то там случилось и срочно нужны деньги? Было такое?*

Скорее всего, его страницу взломали злоумышленники. Они добывают логин и пароль от аккаунта Вконтакте и начинают массово рассылать сообщения по вашим друзьям с просьбой перечислить деньги. Бдительность снижается – ведь вам пишет друг! И люди переводят мошенникам деньги.

1. **Фишинг**

Фишинг: что за улов?

**Фишинг** (от англ. fishing — ловля рыбки) означает, что создается сайт, выглядящий точной копией другого сайта и имеющий похожий адрес (например, вконталке.ру).

Тем или иным способом пользователей интернета заманивают на этот поддельный сайт и предлагают оставить там свой пароль. Так, например, может прийти письмо, которое выглядит в точности как уведомление от ВКонтакте о поступлении комментария к вашей фотографии. Но ссылка на комментарий в письме будет выглядеть примерно так: http://vkontalke.ru/2314. Эта ссылка приведет на поддельный сайт со схожим адресом и очень схожим оформлением. Здесь невнимательный пользователь может оставить свой пароль. Затем человека, как правило, перенаправляют на настоящий сайт, но пароль уже остается у злоумышленника.

1. **Письмо от техподдержки**

Пользователь получает вот такое письмо, пугается, и не опасаясь последствий отправляет свой пароль в руки злоумышленников.

1. **Письмо от банка с тестированием или розыгрышем, получение кредита**

Невнимательные пользователи пройдут по ссылке в письме или отправят свои личные данные.

1. **Отдам в хорошие руки**

Мошенники размещают в группах «Отдам даром» дорогостоящие вещи, которые им якобы не нужны: швейную машинку, Айфон или перфоратор. Нужно только поставить лайк, а владелец сам выберет победителя.

Мошенники пишут всем, кто оставил лайк, поздравляют с победой и просят оплатить доставку. Собирают оплаты за доставку с жертв, удаляют страницу и исчезают.

1. **Продают и обманывают**

Схема та же. Вы оплачиваете товар, частично или полностью и после этого продавец исчезает.

**Как защититься от мошенников?** См. презентацию

**Мошенничество в инстаграм**

***Слайд №17-18***

**Вопрос:**

*- Ребята, поднимите руки, у кого есть аккаунт в инстаграм? Видели фальшивые аккаунты?*

Инстаграм тоже очень популярен среди мошенников. Они могут создавать фальшивые аккаунты или взламывать аккаунты, на которые вы подписаны, чтобы выманивать у вас деньги и личные данные.

**Вот 6 популярных способов инстаграм-мошенничества**

1. Продажа одежды. Онлайн-магазин выглядит достоверно. Хозяева аккаунта публикуют фотографии товаров с выгодной ценой, заманивают большими скидками и уникальными предложениями. Много подписчиков и комментариев. Но их, как вы знаете, несложно накрутить. Проверьте, принадлежит ли страница реальному магазину, и только после этого покупайте.
2. Услуги гадалки. В этом случае мошенница может наживаться на суеверии людей и на их отчаянном положении. Не забывайте, что по ту сторону может скрываться обычный человек, который хочет заработать на вашей проблеме.
3. Услуги гуру. Наставники действительно могут помочь человеку выйти на новый уровень в доходах. Но не обращайтесь к непроверенному «гуру», т.к. вы можете остаться и без наставника и без денег. Выбирайте среди проверенных.
4. Торговля другими товарами. Одной одеждой обманщики не ограничиваются, поэтому можно встретить различные предложения: детские коляски, косметика, товары для животных, электронная техника и т.д. Любой интернет-магазин может оказаться поддельным, особенно, если о нем нет упоминаний в других социальных сетях. Все делается по обычной методике: на аккаунт с большим количеством подписчиков, лайков, комментариев, которые накручены самими мошенниками, вешается объявление от вымышленного магазина, распродающего товары с большой скидкой 50-70%. После переписки люди отправляют деньги на указанный мошенником кошелек, после чего ждут свой товар, а в это время их кормят завтраками и обещаниями. А впоследствии такой мошеннический инстаграмм аккаунт и вовсе удаляется.
5. Ссылки на мошеннические сервисы. В инстаграм очень много аккаунтов, которые обещают огромную прибыль за короткие сроки. Все ссылки ведут на сомнительные сайты, где вы можете потерять большие суммы денег.
6. Фейковые розыгрыши. Когда ТОПовые блогеры в игстаграм проводят крупные Giveaway, мошенники не дремлют. Например, во время giveaway у Тимати с призом 3 000 000 рублей, мошенники запустили рекламу используя видео Тимура для его настоящего гива с целью выудить денег у доверчивых пользователей. Участникам предлагали пройти небольшой опрос и получить за это десятки и сотни тысяч рублей. Мошенники выуживают небольшие суммы от 200 до 400 рублей через «комиссии», «закрепительные платежи или «сервисные сборы».

**Будьте внимательны в следующих случаях** См. презентацию

**Как защититься?** См. презентацию

**Мошенничество в Tik Tok**

***Слайд №19***

Социальная сеть TikTok – это новый Vine и Instagram в одном. Само приложение TikTok появилось в 2016 году в Китае. За 500 дней оно побороло крупных конкурентов внутри страны. Аудитория сервиса к началу 2018 года составила 300 миллионов человек.

Основная аудитория TikTok в России — подростки от 14 лет до 21 года. Но сейчас в TikTokе представлены и крупные известные компании.

В целом в TikTok пока нет такого количества мошенников, как в других соцсетях.

В ТикТок можно перейти только к привязанным аккаунтам в ютуб и инстаграм, активных ссылок на сторонние ресурсы эта соцсеть не дает.

Но все же риск мошенничества существует всегда.

**Как защититься?**

* Не переводите деньги непроверенным блогерам для рекламы вашей страницы.
* Будьте внимательны, если кто-то просит вас продолжить общение за пределами ТикТок, особенно, если собеседник пытаемся вам что-то продать.
* Выбирайте надежные пароли и не давайте доступ к своему аккаунту другим людям
1. **Мошенники в Youtube**

***Слайд №20***

***Вопрос***

*- Ребята, у кого есть свой канал на YouTube?*

*-Вы можете назвать, какие есть способы мошенничества, связанные с YouTube?*

*Давайте разбираться!*

**Способы мошенничества:**

1. **Легкий заработок**

Заинтересовывают жертву роликом с заголовком, в котором предлагают легкий заработок.

В самом ролике показывают, какие именно действия следует выполнить для получения денег. После этого следуют инструкции по оплате одной или нескольких комиссий. А в самом конце демонстрируется успешное получение денег на карту.

Правдоподобные комментарии усыпляют бдительность «жертвы».

**Как защититься?**

1. Не забывайте, что бесплатный сыр бывает только в мышеловке. Никакой волшебной кнопки, чтобы получать деньги «за просто так» не существует.
2. Установите надежный антивирус с защитой от фишинговых и мошеннических сайтов.
3. **Покупка/продажа YouTube-каналов**

При покупке канала есть риск потерять и канал и деньги!

1. **Письма от псевдо-сотрудников YouTube**

Скорее всего, в письме будет говориться о взломе вашего аккаунта и чтобы его защитить, вам нужно перейти по какой-то ссылке.

**Как защититься?**

Тщательно проверяйте адрес отправителя. Если вам пишут специалисты из ютюба, то адрес почты будет официальным \*@youtube.com.

1. **Мошенники в мессенджере Telegram**

***Слайд №21-23***

***Вопрос:***

*- Кто знаком с мессенджером Telegram? Чем он удобен?*

*- А вы знаете, что в телеграм масса различных помощников-ботов и чат-ботов?*

**Что это такое?**  **Бот - это сокращение от слова «робот».**

Бот - автономная компьютерная программа, выполняющая определенные функции.

Всем известен чат-бот «Сберкот» в соцсети Вконтакте от Сбербанка – помощник по финасам для молодежи.

Что еще могут боты? Например, бот может забронировать билеты на концерт или в кино, записать на прием в районную поликлинику и так далее. Другие боты продают различные товары или услуги - от канцелярских ручек до автомобилей, от деда мороза на новый год до уборки квартир.

И вот здесь нужно быть осторожным. Мошенники создают бота-клона, который копирует функционал настоящего, но после оплаты вы ничего не получите.

**Как можно защититься?**

Официальные телеграм-боты оставляют контакты и дают возможность связаться с представителями компании любым другим способом кроме telegram. А ещё вход в бот должен происходить через ваш профиль на официальном сайте. А иные компании оставляют на сайте ссылку на своего бота в telegram.

*Внимание! Если вам пишут личным сообщением с предложением что-то купить, то скорее всего это мошенники. А тем более, если они предлагают купить через бота. Будьте осторожны!*

**Звонки в телеграм**

Чтобы отказаться от рекламных звонков, сделайте следующее: Откройте в приложении telegram “Настройки - Приватность и безопастность - Звонки” и указать кто вам может позвонить:

**Раскрутка канала**

**Вопрос:**

*- Ребята, кто хочет развить свой канал в телеграм до 100 тысяч подписчиков?*

Для этой цели есть масса чатов, где вам предложат купить рекламу в чужих каналах. Если вы натолкнетесь на мошенника, то не получите никакой рекламы и денег тоже вам никто не вернет.

**Как защититься?**

Связь с администратором любого канала и переговоры о покупке рекламы держать только через контакт, который указан в описании канала.

**Телеграм-схемы заработка из даркнета**

Многие ищут в телеграм схемы заработка из даркнета и охотно подписываются на такие каналы. Эти схемы не работают, не тратьте деньги.

**Запуски**

Мошенники работают по стандартной схеме. Сначала открывается канал с годным контентом и автором — бизнесменом. Покупается реклама. В канал выкладывается действительно качественная информация, автор рассказывает о себе и своих планах. Все отлично. Потом аудитория подогревается: автор публикует истории о новом инновационном сервисе, в который он наберёт в дальнейшем лишь 10 человек учеников, или инфопродукте, способному озолотить за минуты. Наступает день или неделя икс. Автор объявляет о наборе учеников, инвесторов, партнёров или продажи уникального курса, методики, пособия для заработка. После успешных продаж воздуха, канал закрывается, умирает или продается.

**Как защититься?**

Прежде чем покупать инфопродукт, узнайте подробно об авторе. Забейте в поисковую строку Яндекса имя и фамилию персонажа - есть ли у него репутация, отзывы, контакты. Не покупайте кота в мешке.

**SCAM Черная метка от команды Дурова**

SCAM в переводе означает "Мошенничество". Такую метку в Телеграме могут получить пользователи, каналы и боты. В предупреждении говориться: многие пользователи сообщили об этом аккаунте, как о мошеннике. Пожалуйста, будьте осторожны, особенно если у вас попросят денег. Если вы увидели такую метку в телеграм, ни в коем случае не платите им деньги за какие-либо услуги.

**Вопросы:**

*- Ребят, знаете ли вы ситуации, когда кто-то другой в Телеграм притворяется другим человеком? Что делать в этом случае?*

**Ответ: Если мошенник притворяется вами, пожалуйста, свяжитесь с @NoToScam.**

**Как можно пожаловаться на мошенников в Телеграме?** См. презентацию

**Подведение итогов**

Мы живем в век бурного развития цифровых технологий. Просыпаемся и засыпаем с телефоном в руке. Роботы – пылесосы убирают наши квартиры. Отдыхая в любом уголке нашей страны или заграницей, мы общаемся сообщениями ил голосом через мессенджеры. Мы заказываем еду и покупаем билеты в кино через мобильные приложения. Технологии неизбежны. Что нас ждем через несколько лет? Какие новые виды денег могут появиться? Какие новые мобильные приложения и социальные сети предложит нам всемирная паутина?

Ясно одно. Мир не будет стоять на месте. И мы должны меняться вместе с ним. Изучать финансовую грамотность, навыки безопасности при пользовании гаджетами и приложениями и уметь защитить себя от финансовых киберпреступников.

***Советы Слайд №24***

***Подведение итогов, вопросы для обсуждения Слайд №25***

***Решение задач, выполнение заданий Слайд № 26-27***

***Спасибо за внимание! Слайд № 28***

***Для преподавателей в качестве домашнего задания можно порекомендовать:***

1. Решение задач
2. Написать эссе: «Как вы представляете себе валюту будущего?»
3. Или подготовить доклад по темам, обсуждаемым на занятии.
4. Устроить дебат-клуб. Например, на тему: «Опасен ли искусственный интеллект?» или «Заменят ли роботы человека в космосе?»