Основы безопасности жизнедеятельности в сети Интернет

Урок 7. Мошенничество в Интернете.

Презентацию подготовила Ванюшина О.А., учитель математики и информатики МБОУ «Ерцевская СШ».

Умение распознавать потенциальные риски в процессе общения в Интернете, предотвращать их и справляться при столкновении с ними, то есть обеспечивать безопасность своей коммуникации в Сети, — важная составляющая коммуникативной компетентности цифрового гражданина.

Ошибки, совершаемые в процессе коммуникации и способные привести к возникновению рискованной ситуации: предоставление персональной информации, открытость профилей, публикация материалов, способных навредить репутации.

Особое внимание необходимо обратить на ключевые коммуникационные риски, связанные с взаимодействием между подростками и другими пользователями в Интернете. К таким рискам относят: общение с незнакомцами, агрессию и сексуальные домогательства.

Как показало исследование цифровой компетентности российских подростков (2013), каждый третий школьник 12–17 лет сталкивался с коммуникационными рисками, которые возникают в процессе общения и межличностного взаимодействия в Сети. При столкновении с каким-либо риском, особенно впервые, дети и подростки зачастую не знают, как поступить.

Под мошенничеством принято понимать хищение имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Основная задача мошенников — втереться в доверие к жертве, чтобы ввести ее в заблуждение и заставить принять необдуманное решение.

Сегодня мошенники активно осваивают информационные технологии, распространяя свою деятельность по всему Интернету. Как правило, интернет-мошенники рассчитывают на неопытность пользователя, привлекая при этом различные технические средства, набор которых постоянно совершенствуется.

Одна из наиболее распространенных форм мошенничества в Интернете — это *фишинг, под которым понимают мошеннические действия или схемы, направленные на получение персональных данных у пользователей.*

Приемы, используемые мошенниками, стары как мир, поэтому компетентный пользователь должен знать их и уметь распознавать.

Рассмотрим основные психологические технологии, используемые интернет - мошенниками.

• *Апелляция к сильным эмоциям*. Поскольку человек в состоянии аффекта утрачивает способность критично воспринимать и оценивать информацию, большинство фишинговых сообщений содержит в себе послание, вызывающее сильную эмоциональную реакцию, например:

✔угрозы здоровью и благополучию близких людей, закрытия банковских счетов, заражения компьютера опасным вирусом.

• *Обещания большой денежной выгоды с минимальными усилиями или даже без них*, например:

✔ беспроигрышная лотерея или неожиданное наследство, сведения о сделках, которые слишком хороши для того, чтобы быть правдой;

• *Запросы о пожертвованиях от лица благотворительных организаций* после сообщений в новостях о стихийных бедствиях.

Несомненно, вы завели много друзей в Интернете, особенно в чатах. Но вы должны быть осторожны. Есть люди, которые заинтересованы в детях и подростках, таких как вы, но совсем не так, как ваши родители. Мы говорим о взрослых, которые используют чаты и притворяются вашими ровесниками, для того, чтобы назначить встречу с вами или сделать вам непристойные предложения.

Поэтому если виртуальный знакомый приглашает тебя на реальную встречу надо (выберите все правильные ответы):

1. *Обязательно пойти.*
2. *Вежливо отказаться.*
3. *Рассказать взрослым.*
4. *Договориться встретиться в удобном для тебя месте, где много людей.*

В Интернете можно переписываться с друзьями, играть с людьми даже по другую сторону Земли, и чатиться с множеством людей одновременно. Но нельзя забывать, что людей, с которыми говоришь, тебе не видно, и есть много воров, мошенников и прочих преступников, которые пользуются чатами и притворяются такими, как вы.

Они могут постараться заставить вас выдать личные данные о себе.

Какую информацию желательно никому сообщать? (выберите все правильные):

1. *Номер телефона.*
2. *Твою годовую оценку по математике.*
3. *Домашний адрес.*
4. *Номер папиной кредитной карточки.*
5. *Кличку твоего попугая*.

Несомненно, вы используете или по крайней мере знаете о программах, которые позволяют чатиться, и называются «клиенты обмена мгновенными сообщениями». Эти чаты отличаются тем, что они приватные и обычно общение происходит только между двумя людьми. Они также позволяют вам вместе с сообщениями слать своим друзьям файлы.

Иногда эти системы используют люди с плохими намерениями, поэтому если твой виртуальный знакомый пришлет тебе файл в подарок надо:

1. *Сразу его открыть.*
2. *Немедленно его удалить.*
3. *Проверить файл антивирусной программой, и если нет вирусов, запустить его.*

Несомненно, вы знаете, что существуют веб-страницы с очень неприятными картинками и текстом, предназначенные только для взрослых, и вы ничего не потеряете, не увидев их.

Такие страницы с взрослыми картинками могут открываться сами собой в случае когда (выберите все правильные ответы):

1. *твой компьютер заражен вирусом;*
2. *такого не может быть;*
3. *вирусом заражен сайт, на который ты хотел попасть;*
4. *«раз в год бывает, что и палка стреляет»*

Объявлений, предлагающих заказать персональный гороскоп, во «Всемирной паутине» очень много. Авторы обещают выслать его быстро и бесплатно. Вам предлагается заполнить стандартную анкету, но вместо гороскопа в его ящик попадает письмо с еще одним условием: чтобы получить заказ, надо отправить по указанному номеру SMS-сообщение с набором тех или иных цифр. Это делается чтобы:

1. *Вас обмануть и взять за отправленную SMS 100 и более рублей.*
2. *Проверить уровень безопасности и не прислать твой гороскоп кому-нибудь другому.*
3. *Переслать тебе гороскоп по SMS.*

Для аферистов, которые не умеют «совершенствовать» банкоматы, придуман самый известный способ мошенничества – интернет-реклама всевозможных мелодий и игр для мобильников. Оплачиваете из интернет-кошелька заказанный дешевый «контент» (песню, игру, и тп.) в неизвестной фирме и:

1. Вам немедленно присылают заказанное.

2. Присылают, то за что Вы заплатили, но через 2 недели.

3. Присылают не одну игру, а две.

4. Вообще ничего не присылают.

Однако помимо возможностей накопления социального капитала в виде интернет - знакомых, такая практика может быть довольно рискованной. Большое количество френдов в социальных сервисах работает на популярность подростка, поэтому многие знакомятся и добавляют в списки друзей всех подряд. Таким образом, они допускают незнакомых людей к своей личной информации и могут подвергнуть себя риску. Как, например, 16-летняя школьница из Голландии, которая забыла установить настройки приватности встречи. Это приглашение было моментально растиражировано, и в результате домой к девушке пришли 4 000 человек.

Такие случаи не редкость: в Гамбурге на день рождения к девочке пришли 1 500 пользователей Facebook, увидевших приглашение, а в США на празднование 15-летия Ребекки Джавело собрались прийти 21 000 пользователей, из-за чего пришлось отменить вечеринку и вызвать отряд полиции для охраны дома.

Настройки конфиденциальности публикаций — необходимая мера для обеспечения безопасности личных данных. Некоторую информацию не стоит публиковать вовсе. Как, например, сделала одна девушка из Австралии: она выложила в социальной сети свою фотографию с пачкой денег.

Это фото заинтересовало преступников, которые вскоре наведались домой к ее матери с ножом и дубинкой. К счастью, женщина не пострадала, а грабителям пришлось довольствоваться небольшой суммой денег, так как фото было сделано в другом доме. Но этот случай показал, насколько опасна может быть необдуманная публикация в Сети.

Доступ случайных интернет - знакомых к личной информации не единственная проблема. Когда общения в Сети становится недостаточно, многие хотят перенести его в реальную жизнь. Как показало исследование «Дети России онлайн», 47 % детей общались в Интернете с кем-либо, с кем они никогда не общались в реальной жизни, а каждый пятый (21 %) лично встречался с интернет - знакомыми. Девочки немного чаще, чем мальчики соглашаются на такие встречи.

Получив подозрительное сообщение, его нужно как следует обдумать, прежде чем предпринимать какие-либо действия.

- Нужно обратить внимание на источник сообщения: как правило, фишинговые сообщения приходят с незнакомых или подозрительных адресов.
- Информацию всегда следует перепроверять, например связаться с отправителем по телефону, посмотреть официальный веб-сайт или найти информацию в любом поисковике.
- Если информация в сообщении содержит угрозу для жизни и здоровья близких людей, которых сейчас нет рядом с вами, стоит подумать, где и с кем они могут сейчас быть.
- Имеет смысл обратить внимание на само сообщение: как правило, оно содержит грамматические и стилистические ошибки, недопустимые при деловой переписке.
- Обычно фишинговое сообщение содержит в себе массу неточностей и противоречий, которые легко можно найти при спокойном и трезвом подходе.