Исследовательский проект

«Обман в сети Интернет»

Выполнили: Шпак Александр, ученик 11 класса

Насыров Абдулатиф, ученик11 класса

Проблемный вопрос

Какие правила необходимо соблюдать, чтобы не попасться на уловки мошенников в Интернете?

Гипотеза исследования

Избежать обмана в сети Интернет возможно в случае хорошей информированности пользователей сети Интернет.

Цели исследования

- Ознакомление учеников нашей школы и их родственников с основными видами мошенничества в сети Интернет.

- Создание Памятки с рекомендациями безопасного использования ресурсов сети Интернет.

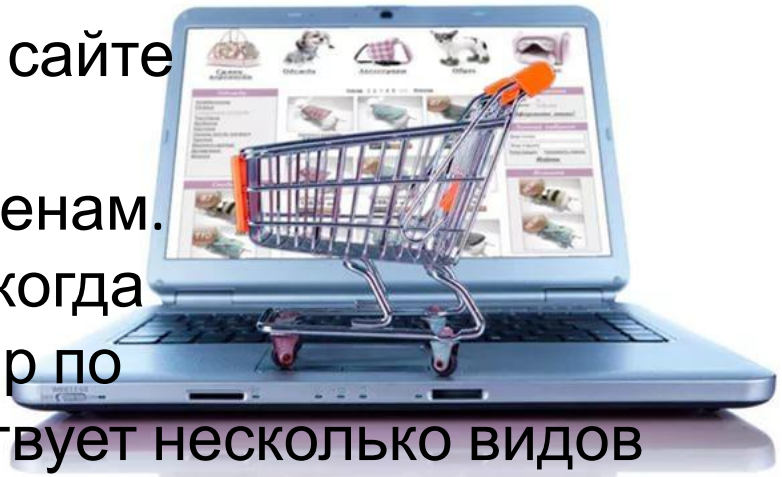
Этапы работы

- Рассмотреть основные виды мошенничества в сети Интернет.
- Провести анкетирование «Встречались ли Вам попытки виртуального мошенничества?» .
- Проанализировать результаты анкетирования.
- Создать буклет с рекомендациями безопасного пользования ресурсами сети Интернет.
- Распространить буклеты среди обучающихся, родителей и учителей школы.

Каким бывает мошенничество в Интернете?

Виды мошенничества в интернете — это огромная проблема для современного мира. Дело в том, что компьютеры и всемирная паутина становятся основными источниками хорошего дохода людей. Таким образом, мошенники используют разные ходы, чтобы «развести» честных граждан. Давайте посмотрим, с чем можно столкнуться и как не напороться на обман в Интернете.

Интернет-магазины



Мошенничество в Интернете довольно часто начинается с интернет-магазинов. На сайте какого-либо магазинчика вам будет предложено купить товар по низким ценам. Особенно привлекательно это тогда, когда Вы можете купить эксклюзивный товар по заниженной стоимости. Далее существует несколько видов «развода». Первый и самый откровенный — это оплата покупки полностью или предоплата до получения. После того как вы перечислите деньги на счет мошенника, он просто исчезает и не выходит на связь. Любые попытки связаться с администрацией терпят фиаско. Второй исход менее неприятный. Вы оплачиваете покупку, а взамен получаете или подделку, или какую-нибудь ерунду, которую вы и вовсе не заказывали. И снова все попытки связаться с продавцом терпят неудачи.

Попрошайки

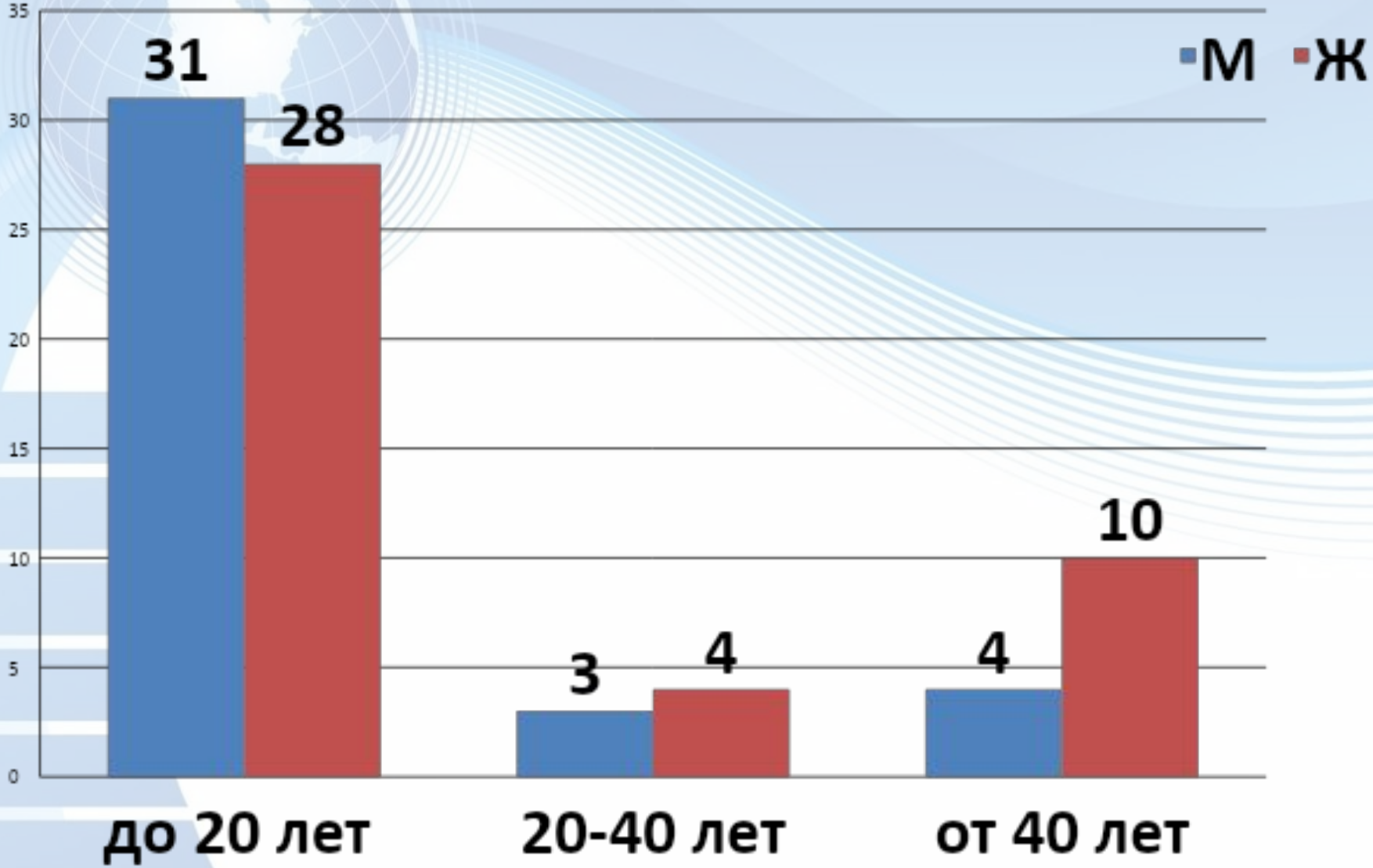
Попрошайничество в Интернете — это
совсем не то, о чем вы думаете. Никто н
станет писать вам с просьбой «подайте
пропитание». Здесь все устроено гораз
хитрее. На сайтах или социальных сет
размещаются объявления с просьбами
помочь больному ребенку или сироте.
Естественно, никто не станет скупиться ради спасения жизни бедняжки-малыша. В объявлении, как правило, указываются все данные для связи и лицевой счет, на который нужно переводить денежную сумму. Вы перечисляете деньги, надеясь, что спасаете жизнь ребенку. Но на самом деле, вы просто пополняете счет какому-то мошеннику. Хорошенько подумайте, прежде чем переводить деньги. Иногда мошенники слишком хорошо готовятся к своему делу.

ФИШИНГ

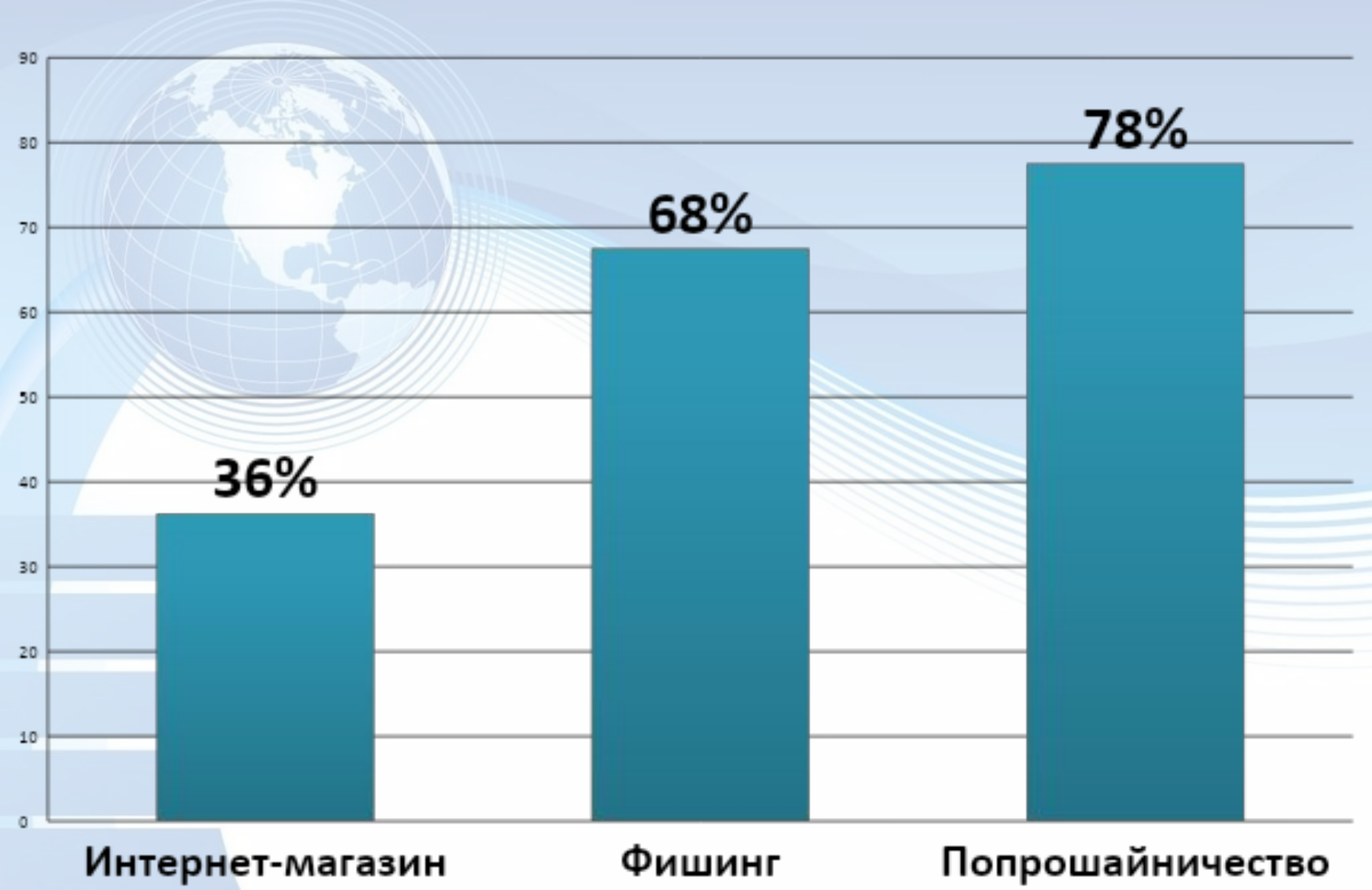
Цель данного занятия — это получение данных вашей пластиковой карточки.

От вас попросят ввести ваши данные с карточки, так как,
скажем, меняется система оплаты и обналичивания средств. После того как вы закончите ввод, вся информация поступит мошеннику. С каждым годом подобные «разводы» развивают новые виды мошенничества в Интернете, что позволяет учитывать злоумышленникам свои старые «ошибки». Так что никогда не переходите по подозрительным ссылкам, присланным вам по электронной почте. И уж тем более не указывайте никаких своих данных.

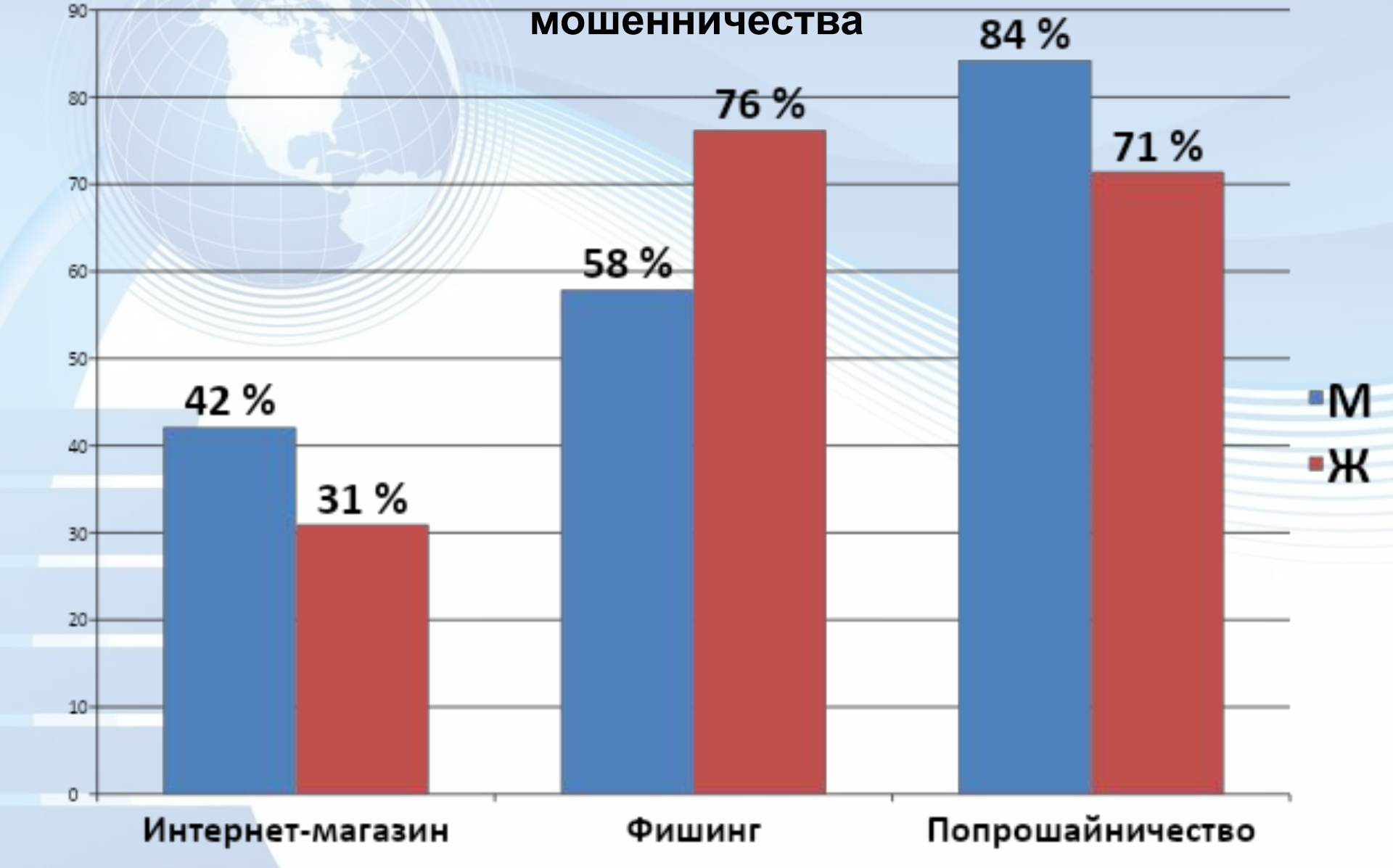
Количество людей, принявших участие в анкетировании



Количественное соотношение ответов респондентов


90
80
70
60
50
40
30
20
10
0
36%
68%
78%
Интернет-магазин
Фишинг
Попрошайничество

Процентное соотношение мужчин и женщин, которые сталкивались с различными видами сетевого мошенничества



Выводы:

- 100 % респондентов хоть раз в жизни сталкивались с виртуальными мошенниками.
- Чтобы работа в сети Интернет была безопасной, необходимо знать и соблюдать определённые правила.
- Необходимо познакомить с этими правилами как можно большее число людей.

Рекомендации безопасного пользования ресурсами сети Интернет

Не дайте себя обмануть!

Запомните основные признаки мошенничества в Интернете:

- Слишком сладкие обещания, например, вам предлагают получать нереально высокий доход за какую-то ерундовую работу.
- Отсутствие контактных данных на сайте для обратной связи, иногда они есть, но не действуют.
- Сайт, предлагающий Вам высокий дополнительный доход, сам расположен на бесплатном хостинге.
- Заманчивое предложение пришло к Вам на почтовый ящик в виде СПАМа.
- Просьба выслать или перевести на электронный кошелёк деньги за регистрацию, за инструкции, за почтовые расходы и т. п.
- SMS-оплата на короткий номер. В результате с баланса Вашего телефона снимут сумму в несколько сотен.

Делаем выводы:

- Не отправляйте СМС на короткие номера, не узнав прежде их реальную стоимость! Не оставляйте номер своего мобильного на сомнительных сайтах!
- Всегда проверяйте контактные данные, представленные на сайте компании или частного лица, с которыми планируете иметь дело.
- Проверьте регистрационные данные самого сайта, на какую компанию или частное лицо было зарегистрировано доменное имя и как давно.
- Если Вам предлагают работу, то платить должны Вам, а не Вы. Не отправляйте деньги за регистрацию, за почтовые расходы, как залог за комплектующие, с которыми Вам предстоит работать и т. п.
- Почитайте отзывы других пользователей сети об этой компании, сайте или частном лице.

Буклет с рекомендациями

Не дайте себя обмануть!
Запомните основные признаки мошенничества в Интернете:

- Слишком сладкие обещания, например, вам предлагают получать нереально высокой доход за какую—то ерундовую работу, которая не займёт у вас много времени и не требует особых знаний и умений.
- Отсутствие контактных данных на сайте для обратной связи, иногда они есть, но не действуют.
- Сайт, предлагает Вам высокий доход, сам расположен на бесплатном хостинге.
- Просьба выслать или перевести на электронный кошелёк деньги за регистрацию или инструкции.
- SMS—оплата на короткий номер. В результате с баланса Вашего телефона снимут сумму в несколько сотен, хотя на сайте чаще всего заявлена сумма в пределах двух—трёх десятков рублей, а где—то внизу мелким–мелким шрифтом что то невнятное, типа: стоимость услуги узнавайте у своего оператора связи.

Делаем выводы:

- Не отправляете СМС на короткие номера, не узнав прежде их реальную стоимость! Не оставляете номер своего мобильного на сомнительных сайтах!
- Всегда проверяйте контактные данные, представленные на сайте компании или частного лица, с которыми планируете иметь дело.
- Проверьте регистрацию данных самого сайта.
- Если Вам предлагают работу, то платить должны Вам, а не Вы. Не отправляете деньги за регистрацию, за почтовые расходы, как залог за комплектующие, с которыми Вам предстоит работать.
- Прочитайте отзывы других пользователей сети об этой компании, сайте или частном лице.

Авторы буклета:
ученики 11 класса
МБОУ Часцовской СОШ

Шпак А.
Насыров А

КАК ИЗБЕЖАТЬ МОШЕННИЧЕСТВА В СЕТИ ИНТЕРНЕТ

Февраль
2023

РЕКОМЕНДАЦИИ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ СЕТИ ИНТЕРНЕТ

Виды мошенничества в Интернете — это огромная проблема для современного мира. Дело в том, что компьютеры и всемирная паутина становятся основными источниками хорошего дохода людей. Таким образом, мошенники используют разные ходы, чтобы развести честных граждан. Давайте посмотрим, с чем можно столкнуться и как не напороться на обман в Интернете.

ФИШИНГ

Цель данного занятия — это получение данных Вашей пластиковой карточки. От вас попросят ввести Ваши данные с карточки, так как, скажем, меняется система оплаты и обналичивания средств. После того как Вы закончите ввод, вся информация поступит мошеннику. С каждым годом подобные «разводы» развивают новые виды мошенничества в Интернете, что позволяет учитывать злоумышленникам свои старые «ошибки». Так что никогда не переходите по подозрительным ссылкам, присланным вам по электронной почте!

ИНТЕРНЕТ—МАГАЗИНЫ

Мошенничество в Интернете довольно часто начинается с Интернет-магазинов. На сайте какого-либо магазинчика Вам будет предложено купить товар по низким ценам. Особенно привлекательно это тогда, когда Вы можете купить эксклюзивный товар по заниженной стоимости. Далее существует несколько видов «развода». Первый и самый откровенный — это оплата покупки полностью или предоплата до получения. После того как Вы перечислите деньги на счет мошенника, он просто исчезает и не выходит на связь. Любые попытки связаться с администрацией терпят фиаско. Второй исход менее неприятный. Вы оплачиваете покупку, а взамен получаете или подделку, или какую-нибудь ерунду, которую Вы и вовсе не заказывали. И снова все попытки связаться с продавцом терпят неудачи.

Пользуйтесь проверенными ресурсами!

ПОПРОШАЙКИ

Попрошайничество в Интернете — это совсем не то, о чем Вы думаете. Никто не станет писать вам с просьбой «подайте на пропитание». Здесь все устроено гораздо хитрее. На сайтах или социальных сетях размещаются объявления с просьбами помочь больному ребенку или сироте. Естественно, никто не станет скупиться ради спасения жизни бедняжки-малыша. В объявлении, как правило, указываются все данные для связи и лицевой счет, на который нужно переводить денежную сумму. Вы перечисляете деньги, надеясь, что спасаете жизнь ребенку. Но на самом деле, Вы просто пополняете счет какому-то мошеннику. Хорошенько подумайте, прежде чем переводить деньги. Иногда мошенники слишком хорошо готовятся к своему делу.

Перечень информационных ресурсов

- Бизнес статьи » Каким бывает мошенничество интернете? https://businessman.ru/new-kakim-byvaet moshennichestvo-v-internete.html
- Способы обмана в глобальной сети http://consumersjournal.org/moshennichestvo/sposoby -obmana-v-globalnoj-seti.html
- Общие рекомендации по безопасному использованию интернета и мобильной связи http://interneshka.org/students/gen_saf_rec.php
- Безопасный Интернет (рекомендации родител http://pcenter-tlt.ru/bezopasny-internet
- Поисковая система Яндекс. Картинки https://yandex.ru/images/