Основы мобильной безопасности

Сейчас почти у каждого человека есть мобильный телефон, не исключая детей. Новое модное веяние – это подключение услуги доступа в сеть Интернет с мобильного телефона. Ребенок, имея мобильный телефон всегда и везде с собой, бесконтрольно может использовать его тогда, когда взрослый не может проследить за ним. Также, есть риск получения негативной информации и контента путем получения смс или ммс сообщений.

Крупные мобильные операторы на своих сайтах дают разного рода рекомендации и предлагают ряд уроков по защите своего мобильного телефона. Около 10 млн. пользователей мобильной связи в той или иной степени пострадали от действий мобильных мошенников.

Рассмотрим рекомендации одного из провайдеров, компании «Билайн», которая с 2008 года проводит информирование пользователей сотовой связи об угрозах, создаваемых мошенниками, использующие средства сотовой связи для обмана людей и получения финансовой выгоды (программа «Мобильная грамотность» - http://safe.beeline.ru/ - см.Рис.1):

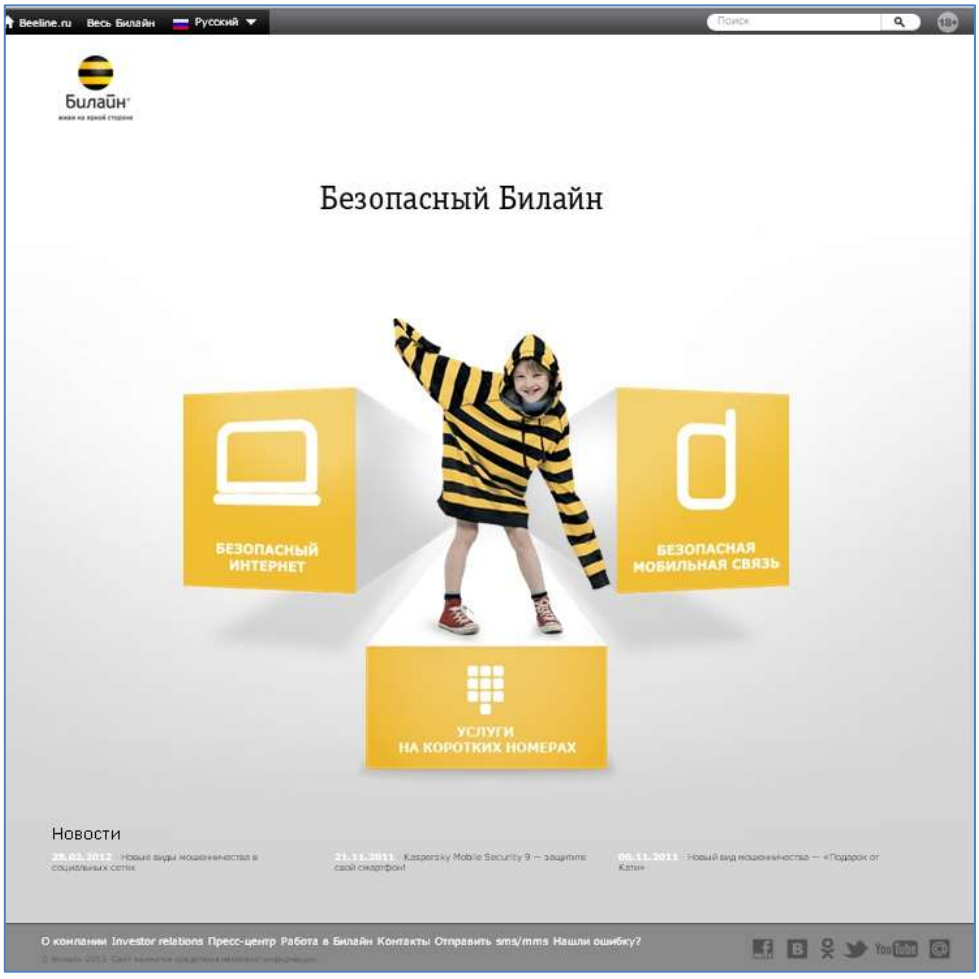

Рис. 1. Сайт компании «Билайн» раздел - Безопасный Билайн.

Приведем некоторые рекомендации от компании «Билайн» по защите своей мобильной безопасности:

— **Убедитесь в достоверности информации**, полученной по телефону от неизвестных, представившихся сотрудниками правоохранительных органов, радиостанции, оператора сотовой связи, чиновниками, вашими родственниками, знакомыми или прочими лицами.

— **Не торопитесь предпринимать действия** по инструкциям неизвестных людей, полученных посредством телефонного звонка или SMS, в особенности, если их инструкции требуют перевода или передачи вами денежных средств каким-либо способом. Позвоните в Центр поддержки клиентов своего оператора и уточните информацию. Поспешные действия могут привести к финансовому ущербу.

— **Не спешите звонить или отправлять SMS на короткий номер,** который обещает разблокировку компьютера от вируса или рекламирует сервис, основанный на доступе к персональным данным других людей. Уточните информацию у своего оператора.

— **Уточняйте у оператора стоимость платных номеров,** предлагающих участие в акциях и викторинах, проводимых контент-провайдерами.

— **Не торопитесь давать телефон** на «1 звонок» незнакомому человеку. Помните, что в последнее время участились случаи краж телефонов именно таким способом.

— **Не открывайте файлы**, пришедшие посредством MMS от неизвестных отправителей, а если есть сомнения - то и от известных. С развитием функциональности мобильных телефонов, корманных персональных компьютеров и коммуникаторов хакеры стали уделять больше внимания созданию вредоносного ПО для этих устройств. По возможности, установите на мобильное устройство одну из многих антивирусных программ, которые вы можете найти на сайтах известных производителей антивирусного ПО.

— **Для разблокировки компьютера от вирусов используйте антивирусное ПО известных разработчиков**, в том числе, бесплатные версии, размещенные на их сайтах. Не стоит верить сообщениям, гарантирующим избавление от вируса или исчезновение интернет-баннера при отправке смс на короткий номер.

— **Вы можете подключить услугу «Черно-белые списки»,** которая позволяет блокировать доступ к сервисам, предоставляемым контент-провайдерами по Вашему желанию. Это позволит Вам более взвешенно относится к пользованию теми или иными сервисами на коротких номерах, а также ограничить доступ детей к нежелательному контенту («взрослые сервисы», импульсивная отсылка смс на CPA–номера под действием рекламы и т.д.) Услуга теперь предоставляется в двух вариантах: создание черного списка номеров (блокировка тех коротких номеров, на которые запрещен доступ с данного номера); создание белого списка номеров (указываются номера, к которым разрешен доступ, все остальные короткие номера блокируются).

Компания «Билайн» принимает активное участие в решении проблемы мобильного мошенничества путем информирования абонентов о существующей угрозе всеми доступными средствами, не только путем размещения информации на их сайте, но и рассылкой смс сообщений.

Раздел «Безопасная мобильная связь» http://safe.beeline.ru/smc/index.wbp знакомит с наиболее популярными схемами мошенничества, рекомендациями и советами. Для самых маленьких пользователей мобильной связи представлены «Уроки мобильной грамотности», подготовленные «Билайн» и «Детским радио». Эти уроки можно прослушать по ссылкам:

Урок 1 «Перенастройка сети»
Урок 2 «Банковская карта заблокирована»
Урок 3 «Звонок с радио»
Урок 4 «Неприятность с сыном»
Урок 5 «Рекламная рассылка - спам»
Урок 6 «Ошибочный перевод денег»
Урок 7 «Компьютерный вирус»
Урок 8 «Благотворительность»
Урок 9 «Новый выгодный тариф»

Вот что предлагает «Билайн» в качестве рекомендаций, чтобы обеспечить мобильную безопасность:

— Если вы считаете, что стали жертвой мошенника, обратитесь в правоохранительные органы и оставьте информацию в абонентской службе своего оператора связи. Ваш мобильный оператор подскажет, что делать, даст нужные телефоны и контакты.

— Если ваш компьютер заблокирован вирусом Troyan Winlock и его модификациями и для разблокировки предлагается отправить смс на короткий номер, обратитесь за помощью к своему интернет-провайдеру или используйте бесплатно **разблокировщик Dr.Web от Trojan.Winlock** и http://support.kaspersky.ru/viruses/deblocker.

— Если у вас нет возможности позвонить в службу технической поддержки для разблокировки компьютера, воспользуйтесь мобильным сервисом разработчика антивирусного ПО "Лаборатория Касперского". При открытии ссылки http://www.kaspersky.ru/news?id=207733379 с мобильного телефона загружается «легкая» версия деблокера.

— Научите детей правильно реагировать на информацию, полученную от незнакомых лиц. «Билайн» и популярная радиостанция для детей «Детское радио» в помощь заботливым родителям запустили совместный образовательный проект - «Уроки мобильной грамотности».

— Дайте послушать детям ряд радио-уроков от Билайн по мобильной грамотности (простом скачайте по ссылкам аудио-файлы

Раздел «Безопасный интернет» http://safe.beeline.ru/si/index.wbp содержит ролик, «Безопасность детей». В данном разделе вы также сможете узнать больше об: угрозах в интернете (Вирус «Trojan.Winlock», Хакеры, Фишинг, Фальшивые антивирусы, Фальшивые главные страницы, и т.д.). Также здесь рассказано о продуктах безопасности и размещены аудио записи «Уроки безопасного интернета», которые можно слушать вместе с детьми. Прослушать записи можно по ссылкам:

Урок 1 «Первая встреча»
Урок 1 (часть 2) «Ошибка на сервере — пришлите пароль...»
Урок 2 «Социальная сеть»
Урок 2 (часть 2) «Новый друг»
Урок 3 «Антивирусные программы»
Урок 3 (часть 2) «Ненужная информация»
Урок 4 «Служба мгновенных сообщений»
Урок 4 (часть 2) «Сплетни и спам»
Урок 5 «Поиск»
Урок 5 (часть 2) «Платные SMS»
Урок 6 «Программы для быстрой работы интернета»
Урок 6 (часть 2) «Компьютерные вирусы»

Некоторые советы от Билайн по безопасному использованию детьми сети интернет:

- Объясните ребенку, почему нельзя предоставлять личную информацию о себе или родителях незнакомым пользователям.
- Объясните, почему нужно быть осторожным при открытии подозрительных писем, страниц, файлов, присланных по электронной почте.
- Расскажите, что люди в чатах не всегда те, за кого себя выдают! Нельзя соглашаться на встречи со своими случайными знакомыми по интернету! Если незнакомец в сети предлагает встретиться, нужно обязательно нужно сказать родителям.
- Держите компьютер дома там, где вам удобнее контролировать его использование.
- Регулярно проводите время в интернете вместе с вашим ребенком.
- Не вините ребенка за неприятные случаи в интернете! Иначе в дальнейшем ребенок станет их скрывать, боясь наказания.
- Попросите показывать все полученные сообщения, особенно, неприятные.
- Приучите ребенка не отвечать на оскорбительные или опасные послания по электронной почте или в чатах.
- Купите специальную программу, которая дает возможность ограничить доступ детей к нежелательным ресурсам. Если

программой будет обнаружен негативный контент, доступ к такой странице сразу блокируется.

Еще один оператор мобильной связи компания «МТС» также информирует своих пользователей о разного вида мобильных мошенничествах, о чем сообщает на своем Интернет-ресурсе по адресу http://www.mts.ru/help/useful_data/safety/ (см.Рис.2):

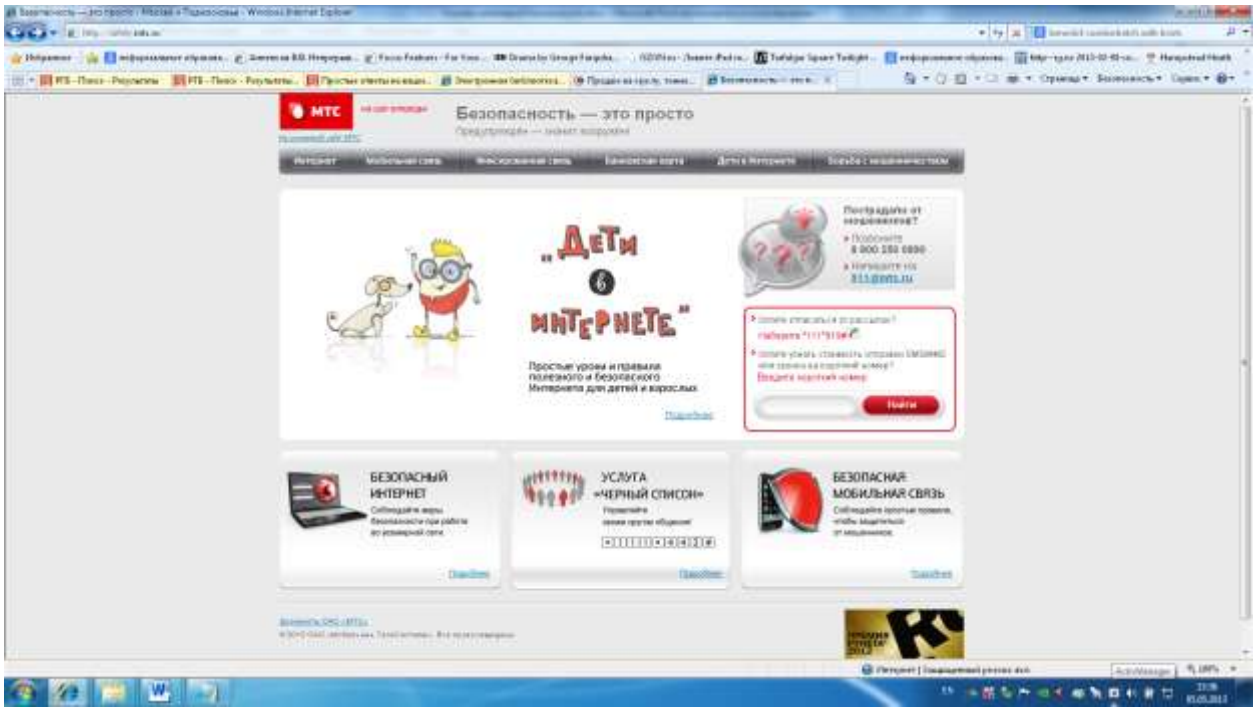

Рис. 2. Сайт компании «МТС», раздел «Безопасность – это просто».

«МТС» предупреждает о видах мошенничества:

— Дорогие SMS на короткий номер. Прежде чем отправить сообщение на короткий номер, узнайте его стоимость с помощью бесплатной услуги «Инфоконтент».

— Кто-то якобы пополнил Ваш счет . Проверьте, пополнился ли Ваш лицевой счет. Помните, что мошенники могут вернуть деньги по чеку в офисе оператора.

— Мошенники выдают себя за сотрудников банка или сотрудников МТС . Не сообщайте никому свои персональные данные или данные своей банковской карты.

— Мошенники из Интернета, компьютерные и мобильные вирусы . Никогда не открывайте сомнительные ссылки в сообщениях или на сайтах. Не открывайте файлы, пришедшие посредством MMS от неизвестных отправителей – это может быть вирус.

— Мошенники обещают призы . Не переводите деньги на чужой счет, не вводите никакие коды на своем телефоне и не отправляйте сообщения на короткие номера, если Вы не принимали участия в лотерее.

— Мошенники просят одолжить телефон. Не одалживайте свой телефон незнакомцам даже «на один звонок» — он может к Вам не вернуться.

— Поздравления от анонима . Не доверяйте поздравлениям от анонимов, не открывайте открытки от неизвестных лиц — Ваши друзья и знакомые вряд ли будут поздравлять Вас анонимно.

— Фальшивые просьбы о помощи от родных и друзей . Не доверяйте просьбам о помощи, не убедившись, что они действительно поступают от Ваших близких.

На сайте есть специальные разделы – для детей и родителей. В разделе для детей, ребенок может посмотреть обучающее видео, поиграть в тематическую игру и даже выполнить задание. В разделе для взрослых приведены основные правила по защите детей.

Ознакомьтесь с разделом «Сервисы МТС для детей и взрослых»:

- **Переключаемые профили**

Ограничить доступ ребенка к нежелательным сетевым ресурсам можно при помощи услуги «Переключаемые профили». Эта услуга позволяет настроить на компьютере профили разного уровня доступа к сети: «Стандартный», «Расширенный» и «Максимальный». Система блокирует определенные порты и протоколы, что гарантирует высокую степень защиты от вредоносного интернет-трафика. Подробнее об услуге фильтрации трафика

- **Ребенок под присмотром**

Чтобы всегда знать, где находится ваш ребенок, воспользуйтесь услугой «Ребенок под присмотром». Эта услуга позволяет отслеживать перемещения ребенка на карте или с помощью SMS по местоположению его мобильного телефона (в том числе через социальные сети). Подробнее об услуге

- **Антивирус и родительский контроль**

Антивирус МТС с функцией родительского контроля позволит защитить ваш компьютер от всех основных видов сетевых угроз. Последняя версия «МТС.Антивирус» разработана совместно с финской компанией F-Secure и обеспечивает защиту от вирусов, сетевых червей и вредоносного ПО; защиту от хакеров; фильтрацию спама и фишинга; защиту детей от нежелательного контента в Интернете (функция «Родительский контроль»). Подробнее о «МТС.Антивирус»

- **Программа фильтрации спама**

Для защиты своего почтового ящика от ненужной рекламы, «писем счастья» и другого спама предлагаем воспользоваться программой «Спамооборона». Компания МТС использует эту программу для защиты

своих пользователей от рассылок спамеров. Подробнее о программе «Спамооборона»

Оператор мобильной связи «Мегафон» также создал специальный раздел «Безопасное общение» http://stopfraud.megafon.ru/ на своем сайте и работает в области защиты от информационного мошенничества (см.Рис.3):

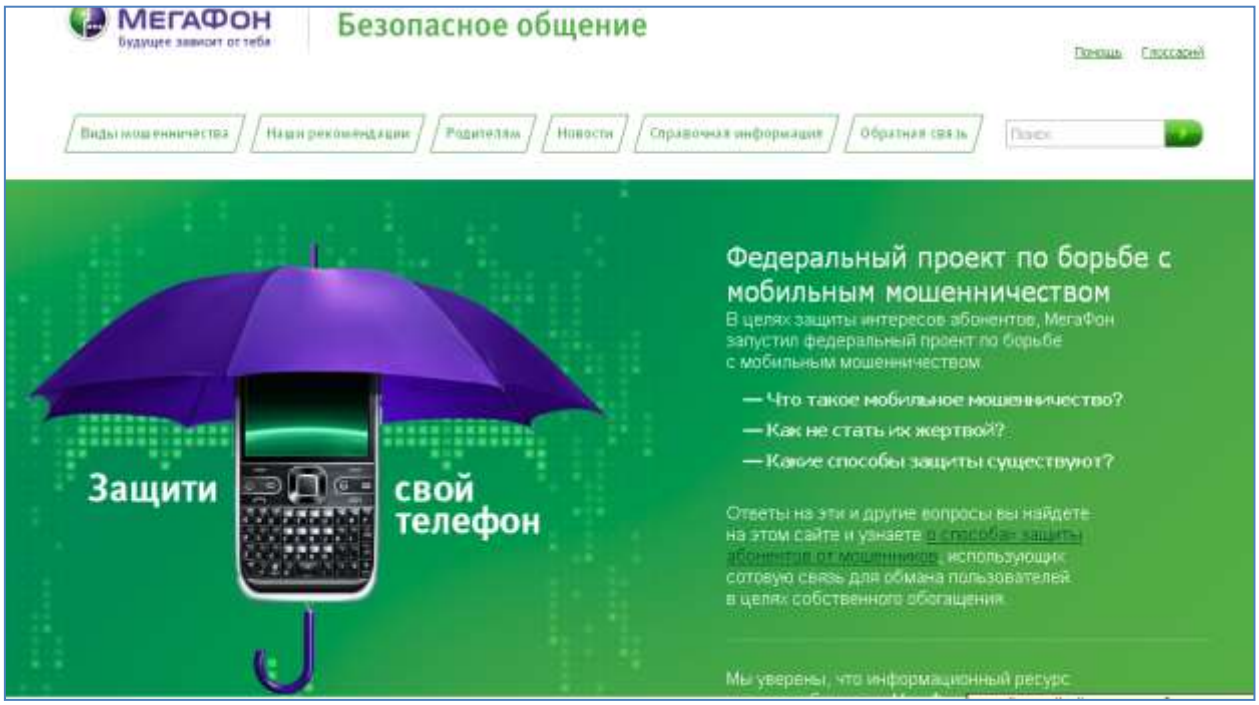

Рис. 3. Сайт компании «Мегафон», раздел – Безопасное общение

Основные виды мошенничества подробно описаны на странице http://stopfraud.megafon.ru/fraudtypes/look.html

По адресу http://stopfraud.megafon.ru/recomendations/ приведены рекомендации компании о том, как не стать жертвами мошенников.

Интересен раздел, адресованный родителям http://stopfraud.megafon.ru/parents/. Вот некоторые рекомендации размещенные в этом разделе:

1. Не размещать на Интернет-ресурсах свой адрес проживания, номер школы, номер мобильного и домашнего стационарного телефонов, адрес электронной почты.
2. Не отправлять свои фотографии и членов своей семьи незнакомым людям, а также видео изображения.
3. Не открывать и не отвечать на спам и на любые письма, пришедшие с незнакомых адресов.
4. Прежде чем общаться с «виртуальными» незнакомцами, советоваться с родителями.

5. Не встречаться без ведома родителей со знакомыми по переписке в Интернете. Помнить, что виртуальные знакомые могут оказаться не теми, за кого они себя пытаются выдавать.

6. Не стесняться спрашивать родителей о незнакомых вещах в Интернете.

Мегафон предлагает также услуги «Родительский контроль» и «Детский Интернет» на компьютере и на мобильном телефоне.

Все вышеперечисленные операторы мобильной связи имеют обратную форму связи, чтобы любой человек мог сообщить о мошенничестве.