

Особый противопожарный режим

В связи с введением на территории объектов жилого назначения города Лесосибирска особого противопожарного режима, инспекторами ОНД по МО г. Лесосибирск совместно с уполномоченными участками полиции, с педагогом-психологом МБУ ЦСОН, сотрудниками дежурных караулов ФГКУ «12 отряд ФПС по Красноярскому краю» проведена агитационно-разъяснительная работа с населением г. Лесосибирска. Вручались памятки о мерах пожарной безопасности, проведены подворные обходы, велась разъяснительная работа. Опубликовано 6 статей, заметок на противопожарную тематику в печатных изданиях, опубликовано 17 статей, заметок на противопожарную тема-

С начала 2015 года на территории города Лесосибирска сложилась непростая обстановка с пожарами и их последствиями. С 10.02.2015 года, постановлением администрацией города Лесосибирска Красноярского края №152 от 06.02.2015 года, на территории объектов жилого назначения города Лесосибирска, введен особый противопожарный режим.

тику на интернет сайтах (В контакте, сайт администрации города), выпущен информационный вестник «Феникс», организовано 2 выступления на телевидение на противопожарную тематику, запущены две социальные рекламы на телевидение «МЧС России предупреждает». Работа, проведенная в рамках особого противопожарного режима, дала результат, обстановка стабилизировалась.

24.02.2015 года на территории г. Лесосибирска отменен особый противопожарный режим в связи с нормализацией пожарной обстановки на

территории объектов жилого назначения города Лесосибирска.

Хотелось бы напомнить гражданам города, что пожар может случиться из-за любой неосторожности в обращении с огнем. И часто бывает так, что случайное действие абсолютно постороннего человека приводит к трагедии для множества людей. Никогда нельзя быть полностью уверенным в безопасности своего жилища, но знайте, что в ваших силах свести вероятность возникновения пожара к минимуму.

Инспектор ОНД по МО г. Лесосибирск ГОРЯЧКИН В.В.



Опасный мобильный вирус для Android

Сотрудники полиции информируют лесосибирцев о том, что в последнее время получает все большее распространение новый мобильный вирус для Android, нацеленный на кражу средств с банковских счетов. Накануне от действия вируса пострадала местная жительница, со счета которой без ее ведома было списано около 3000 рублей.

Полицейские отмечают, что троянская программа под названием Android.BankBot.33.origin распространяется под видом различных полезных приложений для Android и устанавливается на смартфон или планшет только с согласия его владельца. При этом в настройках операционной системы должна быть разрешена установка программ из сторонних источников.

Заразив мобильный гаджет, троянское приложение пытается получить права администратора мобильного устройства, для чего настойчиво демонстрирует соответствующее системное уведомление и фактически не позволяет потенциальной жертве отказаться от выполнения запрошенного действия. Завладев правами администратора, Android.BankBot.33.origin либо выводит сообщение об ошибке, либо демонстрирует интерфейс приложения, за которым «прячется». Помимо этого, троянец удаляет созданный ранее ярлык, чтобы его было труднее обнаружить и удалить.

Совершив эти действия, Android.BankBot.33.origin устанавливает интернет-соединение и передает «хозяевам» информацию о телефоне, а в ответ получает команды на исполнение. Например, вирус может отправлять SMS-сообщения на заданные

номера, загружать и устанавливать приложения, открывать определенные адреса в браузере, а также функционировать в качестве банковского троянца.

Если владелец телефона пользуется услугой «Мобильный банк», вредоносное приложение способно получить информацию о текущем балансе банковского счета, либо списке подключенных к мобильному телефону пользователя банковских карт, отправляя SMS на соответствующие короткие номера, принад-

лежащие различным банкам. Если троянец получит ответ, то при помощи специально сформированных SMS-команд он попытается автоматически вывести доступные денежные средства на принадлежащий злоумышленникам счет. При этом жертва может долгое время оставаться в неведении о произошедшей краже, так как Android.BankBot.33.origin способен перехватить и заблокировать SMS-уведомления о совершенных операциях.

Помимо этого, троянец способен похищать логины и пароли для входа в системы интернет-банкинга, открывая в браузере страницы, похожие на настоящие формы для входа в онлайн-банк. В результате пользователь может лишиться всех своих денег.

По информации отдела уголовного розыска ОМВД России по г. Лесосибирску Евгения ЕВСЕЕВА

Как защитить свой смартфон от вирусов?

- Не включать «режим разработчика».
- Не включать галочку «установка приложений из сторонних источников».
- Устанавливать приложения только из официальных каналов (e.g. Google play, Amazon store etc.).
- Внимательно следить за теми правами, которые приложения запрашивают при установке.
- Использовать защитное ПО.



ных интернет-магазинах, реклама которых, например, у всех на слуху или которыми уже пользовались ваши знакомые.

Прежде чем принять какое-либо решение, посоветуйтесь со своими родными, знакомыми, друзьями. Проявляйте ост-

рожность, и тогда вы сможете уберечь себя от действий мошенников.

По информации ОУР ОМВД России по г. Лесосибирску Евгения ЕВСЕЕВА

Интернет-мошенничество

Полицейские предупреждают: при покупке товара через Интернет будьте осторожны

Полицейские Лесосибирска призывают горожан быть внимательнее и осторожнее при совершении купли-продажи товаров через Интернет. В последнее время участились обращения граждан в полицию с заявлениями о совершенном в отношении них мошенничестве.

Схема мошенничества проста. Злоумышленники на популярных интернет-сайтах и страницах социальных сетей размещают объявления о продаже товара, как правило, по сниженной цене. Покупатель (потерпевший) соглашается купить у продавца товар через Интернет. Продавец просит оплатить товар (внести предоплату) путем перечисления денежных средств, используя банковскую карту либо денежные переводы. Обещанный товар покупателю не доставляется.

Ситуация намного осложняется, когда цель аферы — хищение денег с кредитных или банковских карт потенциальных покупателей. В этом случае сумма причиненного ущерба не ограничивается только суммой «покупки»: с кредитной карты будут похищены все деньги. В данном случае на сайте фальшивого магазина может действовать специальная программа или код, запоминающий реквизиты кре-

дитной карты жертвы.

Такая схема мошенничества обычно имеет один или несколько явных признаков:

- предлагаемый товар продается по сравнительно низкой цене;
- продавец просит, чтобы была произведена предоплата;
- продавец может длительное время «обрабатывать» жертву - для убедительности высылает на

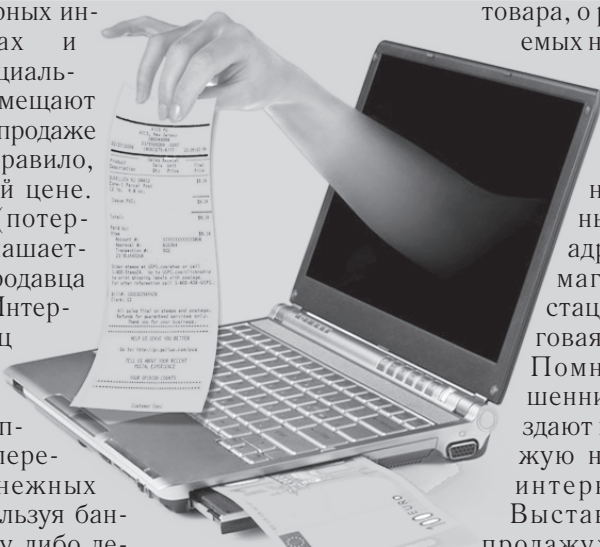
портале на форумах.

На сайте хорошего интернет-магазина обязательно должен быть указан один или несколько контактных телефонов. Рекомендуется позвонить по этому телефону и побеседовать с представителем магазина (например, спросить его о том, как давно на рынке работает данный магазин, задать пару вопросов об ассортименте товара, о распространяемых на товар гаран-

тиях, и т.д.). Постарайтесь узнать, где находится не виртуальный, а «живой» адрес интернет-магазина (офис, стационарная торговая точка, и т.п.). Помните, что мошенники, часто создают витрину, похожую на настоящий интернет-магазин. Выставляться «на продажу» может все, что угодно — как и в любом другом интернет-магазине. Разница заключается в том, что цены, как правило, являются весьма привлекательными.

Если вы ничего об указанном сайте и предлагаемых им товарах не нашли, лучше от предложения отказаться, каким бы заманчивым оно ни казалось. Помните: именно низкая цена должна насторожить вас как потенциального покупателя.

Сотрудники полиции рекомендуют совершать покупки только в извест-



электронную почту покупателя «копии» своих документов (водительского удостоверения или паспорта), старается подружиться, найти общие интересы, войти полностью в доверие, а также в переговоры могут быть привлечены третьи лица.

Поэтому при покупках через Интернет необходимо соблюдать меры предосторожности. Прежде чем приобрести понравившуюся вещь через неизвестный сайт, проверьте информацию об этом ресурсе, о его товарах, поищите и почитайте отзывы о