

# Как обезопасить себя от IT-мошенничества!

## Меры предосторожности при использовании пластиковых карт

В последнее время наблюдается рост числа мошенничеств с пластиковыми картами. Для того, чтобы обезопасить Ваш счет от преступных посягательств, необходимо знать и выполнять следующие простые правила:

1. Никогда и никому не сообщайте ПИН-код Вашей карты. Лучше всего его запомнить, а не хранить рядом с картой и тем более не записывать ПИН-код на нее.

2. Не позволяйте никому использовать Вашу пластиковую карту.

3. Если Вам позвонили из какой-либо организации или Вы получили письмо по электронной почте (в том числе из банка) с просьбой сообщить реквизиты карты и ПИН-код под различными предлогами, не спешите ее выполнять. Позвоните в указанную организацию и сообщите о данном факте. Не переходите по указанным в письме ссылкам, поскольку они могут вести на сайты-двойники.

4. Если Вы утратили карту, срочно свяжитесь с банком, выдавшим ее, сообщите о случившемся и следуйте инструкциям сотрудника банка.

5. При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраной (в государственных учреждениях, банках, крупных торговых центрах и т.д.).

6. Совершайте операции с пластиковой картой так, чтобы находящиеся рядом люди не могли проследить за Вашими манипуляциями. Если это невозможно, снимите деньги с карты позже либо воспользуйтесь другим банкоматом.

7. Обращайте внимание на картоприемник и клавиатуру банкомата. Если они оборудованы какими-либо дополнительными устройствами, то от использования данного банкомата лучше воздержаться и сообщить о своих подозрениях по указанному на нем телефону.

8. В случае некорректной работы банкомата (долгое время находится в режиме ожидания, самопроизвольно перезагружается) откажитесь от его использования.

9. Никогда не прибегайте к помощи либо советам третьих лиц при проведении операций с банковской картой в банкоматах.

10. В торговых точках, ресторанах и кафе все действия с Вашей пластиковой картой должны происходить в Вашем присутствии. В противном случае мошенники могут получить реквизиты Вашей карты при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки.

## **Мошенничество в Интернете**

### **1. Мошенничества, связанные с Интернет-магазинами.**

Через Интернет вам могут предложить приобрести все, что угодно, а распознать подделку при покупке через сеть бывает сложно. Однако, соблюдая некоторые правила предосторожности, можно оградить себя от возможных неприятностей.

Вас должна насторожить слишком низкая цена на определенный товар, а также отсутствие фактического адреса или телефона продавца. Скорее всего, вам предлагают приобрести подделку либо хотят присвоить ваши деньги.

Не поленитесь позвонить продавцу по телефону и подробнее выяснить уже известные вам особенности товара, его технические характеристики и т.д. Заминки на другом конце провода или неверная информация, которую вам сообщили, должны стать поводом для отказа от покупки в данном Интернет-магазине.

Наведите справки о продавце, изучите отзывы о его работе, и только после этого решайте - иметь ли дело с выбранным вами Интернет-магазином.

Пользуйтесь услугами курьерской доставки и оплачивайте стоимость товара по факту доставки.

## **2. Фишинг.**

Фишинг (от англ. fishing - рыбная ловля, выуживание) - вид интернет-мошенничества, цель которого - получить данные, содержащиеся на вашей пластиковой карте.

Злоумышленники рассылают электронные письма от имени банков или платежных систем. Пользователю предлагается зайти на сайт, который является точной копией настоящего сайта банка, где можно увидеть объявления, например, об изменении системы безопасности банка. Для дальнейшей возможности использовать свою пластиковую карту вас просят указать пин-код и данные, содержащиеся на карте. Впоследствии эти данные используются для изготовления поддельной пластиковой карты и обналичивания денежных средств, содержащихся на вашем счете. Оставив свои данные, вы фактически преподносите мошенникам деньги на блюдечке.

Одной из разновидностью данного вида правонарушения являются звонки на сотовые телефоны граждан якобы от представителей банка с просьбой погасить задолженность по кредиту. Когда гражданин сообщает, что никакого кредита не брал, ему предлагается уточнить данные, содержащиеся на пластиковой карте. Этого уже достаточно для покупки товаров в Интернет-магазинах.

Следует помнить, что банки и платежные системы никогда не присылают писем и не звонят на телефоны граждан с просьбой предоставить свои данные. Если такая ситуация произойдет, вас попросят приехать в банк лично.

## **3. Интернет-попрошайничество.**

В Интернете могут появиться объявления от благотворительной организации, детского дома, приюта с просьбой о материальной помощи больным детям. Злоумышленники создают сайт-дублер, который является точной копией настоящего, меняют реквизиты для перечисления денег.

Для того, чтобы не попасться на крючок и не отдать свои деньги в руки мошенников, не поленитесь перезвонить в указанную организацию,

уточнить номер расчетного счета либо посетить ее лично, убедиться в достоверности размещенной информации, выяснить все подробности дела, а затем уже решать - передавать деньги или нет.

#### **4. Мошенничества в отношении иностранных граждан (брачные аферы).**

Не встретив в реальной жизни свою половину, многие мужчины продолжают искать ее в Интернете. Поиски начинаются на сайтах знакомств и дневниках, где будущие избранницы размещают свои фотографии.

Этим пользуются злоумышленники, используя фото девушек, привлекая психологов, программистов, переводчиков и посредством этих сайтов завязывают переписку с доверчивыми иностранцами.

Западные женихи «кдюют» на объявления, где нетребовательные русские красавицы говорят о том, что нуждаются в серьезных отношениях. А взамен вечной любви, порой после месяцев переписки, просят решить их финансовые проблемы - помочь обеспечить сиделкой больных родителей, расплатиться с кредитом, перевести деньги на перелет к жениху в дальнее зарубежье и т.д.

После получения денег невесты перестают выходить на связь. Пылкие иностранные поклонники, поняв, что их обманули, обращаются в полицию. Злоумышленники рассчитывают только на женихов из дальнего зарубежья, т.к. представители ближнего зарубежья предпочитают приехать в гости к невесте сами, что невыгодно для мошенников.

#### **5. Осторожно! Вирус!**

Сущность вируса - переадресация со страницы запрашиваемого ресурса на фиктивную, скопированную с настоящей. Подмена осуществлялась для самых популярных ресурсов Рунета: Яндекс, Рамблер, Майл, ВКонтакте, Одноклассники.

Набирая на «зараженном» компьютере адрес одного из указанных ресурсов, пользователь попадает на сервер-подмену, где ему предлагается страница для входа в систему (имя и пароль). С учетом того, что в адресной строке указано корректное имя, а внешний вид скопирован с оригинального

сервера, у большинства пользователей не возникает подозрений в подлинности страницы.

После ввода имени и пароля отображается иная страница, где уже говорится о необходимости «подтверждения» или «активации» учетной записи за смс на короткий номер, стоимость которого минимальная или якобы бесплатная.

Таким образом, злоумышленники не только снимают денежные средства со счетов абонентов, но и получают логин и пароль доступа пользователя к указанным популярным ресурсам, что позволяет им в дальнейшем отправлять от имени «жертвы» различные сообщения, например:

- программка для бесплатной отправки подарков! мне не забудь отправить!

- привет. Лови программку по бесплатному повышению рейтинга, но не давай никому больше. Это не спам.

Основные темы, которые используются для «рекламы» скачивания и запуска зараженных программ:

- бесплатное повышение рейтинга «ВКонтакте»;

- программа перехвата SMS сообщений с телефона;

- дополнительные функции в социальных сетях, которые не существуют (подарки, VIP-доступ и т.д.)

После перехода по ссылке компьютер пользователя автоматически запускает вредоносную программу.

### Наши рекомендации

Пострадавшим рекомендуется изменить пароль доступа к указанным ресурсам, а также установить версии антивирусных программ с обновленными антивирусными базами.

Следует помнить, что ресурсы популярных сайтов никогда не потребуют от уже зарегистрировавшегося пользователя дополнительной авторизации, тем более за деньги путем отправки смс.

## **6. Осторожно!!! Новый вид мошенничества!!!**

В Российском сегменте сети Интернет стала появляться информация о так называемых «звуковых» наркотиках, якобы оказывающих влияние на бинауральные ритмы человека. Реклама аудионаркотиков осуществляется посредством массовой рассылки писем на электронные почтовые адреса пользователей и на номера в системах быстрого обмена сообщениями. Доступ к прослушиванию аудио-файлов возможен после введения специального цифрового кода, получение которого происходит исключительно после оплаты в виде отправки смс-сообщения. Ресурсы, предлагающие такого рода продукцию, располагаются на площадях зарубежных провайдеров и зарегистрированы по фиктивным анкетным данным.

По мнению специалистов, достичь рекламируемого эффекта посредством звуковых колебаний невозможно. Единственным результатом применения «звуковых» наркотиков являются головные боли, частичная потеря памяти и снижение мозговой активности.

Таким образом, информация о «цифровых наркотиках» - это хорошо спланированная «черная» пиар-компания, способная привлечь новых потенциальных покупателей звуковых файлов, и очередной способ получения денег мошенниками.

## **7. Найдено средство от Trojan.Encoder.20**

Количество вирусов, которыми наводнено пространство всемирной паутины, на сегодняшний день не поддается исчислению.

Одной из вредоносных программ, разработанных и внедренных в Интернет киберпреступниками, стал Trojan.Encoder.20, который является усовершенствованной версией своего предшественника Trojan.Encoder.19.

Новоявленная программа-вымогатель распространяется через сайты со встроенным вредоносным кодом путем скрытой загрузки на компьютер посетителя сайта. Она шифрует все файлы пользователей, после чего

самоликвидируется. При попытке открыть файл на экране появляется сообщение с требованием заплатить от 10 до 89 долларов с помощью SMS за возможность расшифровки информации.

Пользователям, пострадавшим от данного вируса, рекомендуется скачать разработанную компанией «Dr. Web» бесплатную утилиту, которая позволяет уничтожить данный вирус.

## **8. Внимание! Социальные сети - как один из способов вовлечения несовершеннолетних в оборот нелегального порно!**

Социальные сети активно используются злоумышленниками для вовлечения детей и подростков в распространение порнографических материалов с участием несовершеннолетних посредством сети Интернет.

Для этого создается вымышленная анкета (электронная страница), где используются фотосессии и вымышленные данные несовершеннолетних, взятые из различных открытых источников. Таким образом, порноделец маскируется под вид обычного подростка, который в сети Интернет пытается рассказать о себе и найти новых знакомых с общими интересами.

В ходе электронного общения создаются условия, побуждающие подростка направить свои откровенные фотографии. После их получения данные изображения распространяются на тематических форумах, файлообменных системах и фото и видеопорталах.

Зачастую злоумышленнику становятся известны анкетные данные подростка, и тогда происходит так называемый «трóллинг» или травля (размещение в Интернете на форумах, в дискуссионных группах, в вики-проектах провокационных сообщений с целью собственного развлечения и созданием конфликтов между участниками). Это необходимо для установления круга знакомых, учителей и родителей подростка с целью направления им полученных провокационных фотографий.

Общаясь в социальных сетях, помните:

Любой человек, с которым вы познакомились в сети и вступили в переписку, может оказаться всего лишь вымышленным персонажем. Не увидев его воочию, вы никогда не сможете быть уверенными в его реальном существовании!

Информация, направляемая Вами посредством сети Интернет - будь это личные данные, фотографии либо видео - может быть использована против Вас, в том числе в корыстных и преступных целях.

Уважаемые родители! Проинструктируйте Ваших детей об элементарных правилах безопасности в Интернете!

Что такое вредоносные программы и как обезопасить себя в Интернете

Основным источником опасности для пользователей компьютеров были и остаются вредоносные программы, которые с развитием сетевых технологий получили новую среду для своего распространения.

Вредоносные программы - это программы, которые способны самостоятельно, без ведома владельца компьютера, создавать свои копии и распространять их различными способами. Подобные программы могут выполнять самые разнообразные действия, начиная от вполне безобидных "шуток" (типа "гуляющих" по монитору картинок) до полного разрушения информации, хранящейся на дисках компьютера.

В обиходе часто все вредоносные программы называют словом "вирусы", хотя, строго говоря, это не так. Вредоносные программы можно разделить на три группы:

- компьютерные вирусы;
- сетевые черви;
- троянские программы.

Компьютерные вирусы - это программы, которые умеют размножаться и внедрять свои копии в другие программы, т.е. заражать уже существующие файлы. Обычно это исполняемые файлы (\*.exe, \*.com) или файлы, содержащие макропроцедуры (\*.doc, \*.xls), которые в результате заражения становятся вредоносными.

Компьютерные вирусы существуют давно. В последнее же время, когда компьютеры стали объединять в компьютерные сети, подключать к



Интернету, в дополнение к традиционным компьютерным вирусам появились вредоносные программы нового типа: сетевые черви и троянские программы.

Сетевые черви - это вредоносные программы, которые размножаются, но не являются частью других файлов, представляя собой самостоятельные файлы. Сетевые черви могут распространяться по локальным сетям, по Интернету (например, через электронную почту). Особенность червей - чрезвычайно быстрое "размножение". Червь без вашего ведома может, например, отправить "червивые" сообщения всем респондентам, адреса которых имеются в адресной книге Вашей почтовой программы. Помимо загрузки сети в результате лавинообразного распространения сетевые черви способны выполнять опасные действия.

Троянские программы не размножаются и не рассылаются сами, они ничего не уничтожают на Вашем компьютере, однако последствия от их деятельности могут оказаться самыми неприятными и ощутимыми. Задача троянской программы обычно состоит в том, чтобы обеспечить злоумышленнику доступ к Вашему компьютеру и возможность управления им. Все это происходит очень незаметно, без эффектных проявлений. Просто в один "прекрасный день" ваша частная переписка может быть опубликована в Интернете, важная бизнес-информация продана конкурентам, а баланс лицевого счета у интернет-провайдера или в электронных платежных системах неожиданно быстро окажется нулевым или отрицательным.

Советы, как обезопасить себя

## **1. Электронная почта**

Электронная почта - на сегодняшний день один из самых популярных способов распространения вредоносных программ в Интернете.

Обычное сообщение электронной почты - это просто текст, сам по себе он не может быть опасен. Но к сообщению можно прикреплять файл, называемый файлом вложения или файлом присоединения, который вполне может оказаться вредоносной программой или зараженным вирусом файлом.

Вредоносные программы - это так или иначе исполняемые файлы (самостоятельные или командные (скрипты)), которые срабатывают при

выполнении на данном компьютере. Можно сформулировать следующую тактику в борьбе с ними:

- во-первых, не допускать, чтобы вредоносные программы попадали на Ваш компьютер;

- во-вторых, если уж они к Вам попали, ни в коем случае не запускать их на выполнение;

- в-третьих, если они все же запустились, принять меры, чтобы, по возможности, они не причинили ущерба.

Если Вы получили сообщение с вирусом, значит, Вы уже невольно выполнили первый предварительный шаг на пути к заражению Вашего компьютера, поскольку опасный файл сохранился на жестком диске. Пока это не фатально, но очень опасно, поэтому, прежде всего, необходимо предпринять меры к тому, чтобы этого не происходило впредь.

У многих операторов связи имеются на почтовых серверах ряд фильтров, отсекающих подозрительные послания. Однако, несмотря на очевидную эффективность общесистемного фильтра, для обеспечения безопасности его все-таки недостаточно, поскольку он рассчитан на обезвреживание уже известных вирусов, тогда как новые вирусы все еще могут беспрепятственно попадать в почтовый ящик. Поэтому пользователю необходимо предпринять дополнительные меры безопасности.

Самый действенный способ оградить от вредоносных программ свой почтовый ящик - это запретить прием сообщений, содержащих исполняемые вложения. Если абонент включает подобный фильтр, то все сообщения, содержащие исполняемые файлы, будут автоматически удаляться непосредственно на почтовом сервере. Несмотря на кажущуюся радикальность подобной меры, она очень эффективна и в большинстве случаев не приводит к неудобствам или ограничениям возможностей пользователей. Во-первых, как правило, по электронной почте чаще всего рассылают документы и изображения, но не программы; во-вторых, при необходимости получить по почте программу можно договориться с отправителем, чтобы он предварительно упаковал ее с помощью какого-либо архиватора, например, Winzip или WinRar. Польза получится двойная, поскольку размер полученного файла-архива должен быть гораздо меньше размера исходного файла.

Имеется еще один способ не сохранять подозрительные сообщения на своем компьютере. Идея состоит в том, чтобы сначала получать с сервера и просматривать только заголовки сообщений и удалять ненужные письма непосредственно на сервере, не скачивая их на свой компьютер. Для этого можно использовать специальные программы.

Если же обстоятельства таковы, что Вы не можете организовать работу так, чтобы не получать сообщения с исполняемыми файлами, а значит, сообщения с вредоносными программами могут быть Вами получены, то необходимо предпринять меры к тому, чтобы вредоносные программы ни в коем случае не были запущены на выполнение.

Для того чтобы запустить файл вложения на выполнение, следует открыть сообщение в отдельном окне, дважды щелкнув на строке сообщения в списке (сообщение с вложением помечено скрепкой) и открыть файл-вложение, дважды щелкнув на имени файла в заголовке сообщения (поле "Присоединить").

Учитывая сказанное, необходимо взять за правило не открывать сообщение (дважды щелкнув мышкой), особенно если сообщение пришло от неизвестного отправителя. Прочитать текст всегда можно в режиме быстрого просмотра (когда при одиночном щелчке мышкой на сообщении в списке текст сообщения отображается не в отдельном, а в основном окне программы). Все подозрительные сообщения немедленно удаляйте.

Также никогда не открывайте немедленно присланные файлы-вложения, в том числе файлы от друзей, коллег или присланные от имени известных фирм. Принимайте во внимание, что сообщения якобы от знакомых лиц могут оказаться рассылками, отправленными сетевыми червями. Также имейте в виду, что без Вашего ведома ни одна уважаемая организация не будет рассылать файлы, даже если это важные данные, такие, как обновления системы или очередная защита от вирусов.

Обращайте внимание на расширение файла. Особую опасность могут представлять собой файлы со следующими расширениями:

-ade adp bas bat;

-chm cmd com cpl;

-crt eml exe hlp;

-hta inf ins isp;

-jse lnk mdb mde;

-msc msi msp mst;

-pcd pif reg scr;

-sct shs url vbs;

-vbe wsf wsh wsc;

Часто вредоносные файлы маскируются под обычные графические, аудио- и видеофайлы. Для того чтобы видеть настоящее расширение файла, обязательно включите в системе режим отображения расширений файлов.

Будьте очень осторожны при получении сообщений с файлами-вложениями. Подозрительные сообщения лучше немедленно удалять.;

Для того чтобы удалить сообщение в почтовой программе полностью:

- удалите сообщение из папки Входящие;

- удалите сообщение из папки Удаленные;

- выполните над папками операцию "Сжать" (Файл/Папка/Сжать все папки).

К сожалению, необходимо отметить, что даже при твердом намерении не открывать немедленно присылаемые файлы нельзя исключать случаи, когда они все-таки будут запущены: вследствие ошибки программного обеспечения, по ошибке или недоразумению. Однако и в этих условиях возможно предпринять контрмеры.

В первую очередь следите, чтобы у Вас были установлены самые последние обновления программ.

Нелишним будет установить персональный межсетевой экран (firewall). В ней следует указать исчерпывающий список программ и доступных им портов и сервисов. Как только какая-либо незнакомая программа попытается отправить почту, она тут же будет обнаружена, и зараза не распространится с Вашего компьютера дальше.

Кроме того, отслеживать и блокировать опасные действия, которые могут выполнять вредоносные программы (обращение к файлам, загрузочной области диска, системному реестру и т.п.), способны специальные программы-сторожа, обычно входящие в состав антивирусных пакетов. Такие программы обычно автоматически запускаются на выполнение при загрузке операционной системы и незаметно прослеживают действия программ.

Наконец, рекомендуем больше внимания обращать на то, что происходит на Вашем компьютере во время сеанса связи с Интернет. Если Вы заметите, что в то время, когда Вы не выполняете никаких действий с сетью, индикатор активности передачи данных по сети говорит об обратном, немедленно прекращайте связь и проверяйте свой компьютер антивирусными программами. Индикатором активности работы с сетью может служить внешний модем (лампочки мигают), значок двух соединенных компьютеров, появляющийся при установлении связи внизу на панели задач (мигает).

#### Рекомендации по обеспечению безопасной работы в Интернете

Суммируя все сказанное, кратко можно сформулировать следующие рекомендации, направленные на повышение безопасности работы пользователя в Интернете:

- установить антивирусное программное обеспечение с самыми последними обновлениями антивирусной базы. Проверять новые файлы, сохраняемые на компьютере. Периодически проверять компьютер полностью.

- отслеживать появление новых версий операционных систем и своевременно устанавливать обновления к ним, устраняющие обнаруженные ошибки.

- настроить операционную систему так, чтобы обеспечивались основные правила безопасности при работе в сети. По возможности отказаться от использования старых операционных программ в пользу более современных.

- регулярно обновлять пользовательское программное обеспечение для работы в сети, такое, как Интернет-браузер, почтовые программы, устанавливая самые последние обновления.

- выполнить настройки почты, браузера и клиентов других используемых сервисов, уменьшающие риск воздействия вредоносных программ и подверженность сетевым атакам.

- никогда не устанавливать и не сохранять файлы, полученные из ненадежных источников: скаченные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях, - без предварительной проверки антивирусной программой. Подозрительные файлы лучше немедленно удалять.

- при получении извещений о доставке почтовых сообщений обращать внимание на причину и в случае автоматического оповещения о возможной отправке вируса немедленно проверять компьютер антивирусной программой.

- по возможности, не сохранять в системе пароли (для установки соединений с Интернетом, для электронной почты и др.), периодически их менять. Регулярно выполнять резервное копирование важной информации.

- подготовить и иметь в доступном месте системный загрузочный диск. В случае подозрения на заражение компьютера вредоносной программой загрузить систему с диска и проверить антивирусной программой.

*Внимание! В социальных сетях орудуют мошенники!*

В период новогодних праздников и в настоящее время в социальных сетях многим пользователям приходят сообщения от посторонних лиц или от друзей, находящихся в контактном листе, с просьбой посетить определенный ресурс или проголосовать за них, отправив смс на короткий номер. Наряду с

этим мошенники зачастую меняют статус пользователей и размещают необходимую им информацию.

Управление «К» предупреждает: не поддавайтесь уловкам мошенников, посещая указанные ресурсы или отправляя смс на обозначенный номер! Вероятнее всего, страница пользователя, от которого приходят подобного рода сообщения, взломана, и от его имени осуществляется массовая рассылка. При переходе на указанные ресурсы велика вероятность заразить компьютер какой-либо вредоносной программой, а после отправки смс на указанный номер можно потерять со счета немалую сумму денег.

Во избежание несанкционированного доступа к вашим страницам в социальных сетях, в том числе и к содержимому электронной почты, а также для предотвращения возможных последствий, связанных с действиями мошенников, следует предпринять следующие меры:

1. Воздержитесь от выполнения указанной в сообщении просьбы.
2. Свяжитесь с другом, от которого вы получили вышеуказанное сообщение, и уточните у него, действительно ли он является автором послания.
3. Если выяснится, что страница пользователя взломана, ему необходимо поменять пароли в социальных сетях и электронной почте, а также проверить компьютер на наличие вирусов.

А в качестве общей рекомендации специалисты Управления «К» советуют пользователям устанавливать на свой компьютер хорошо зарекомендовавшие себя антивирусные программы и не пренебрегать мерами безопасности во время пользования Интернетом.

Остерегайтесь предложений об установлении местонахождения человека по номеру его мобильного!

В последнее время многие пользователи Интернета сталкиваются с размещенной в сети информацией о том, что они могут установить местонахождение человека по номеру его мобильного телефона. Для этого требуется отправить sms с набором определенных цифр на указанный номер и за 10 рублей получить код доступа к услуге.

Однако после проведения вышеуказанных манипуляций клиенту так и не удастся осуществить поиск интересующего его человека, зато с его счета списывается кругленькая сумма.

Управление «К» МВД России предупреждает, что определить местонахождение человека по номеру мобильного телефона можно исключительно с его согласия. Такую услугу предоставляют некоторые операторы сотовой связи в установленном порядке. Однако если подобное предложение исходит не от оператора сотовой связи, а от третьих лиц, то это является не чем иным, как мошенничеством!

Источник информации: <https://ako.ru/deyatelnost/mery-po-profilaktike-moshennichestva-sredi-grazhdan/obshchaya-informatsiya.php>