«Киберпреступность — очень доходный бизнес»

*По данным экспертов, за 2012 год интернет-мошенники во всем мире заработали 21 миллиард долларов, а годом ранее прибыль составила около 12 миллиардов — то есть всего за год их доходы выросли почти в два раза. Это гигантские суммы, сравнимые с запланированными бюджетными тратами России, скажем, на здравоохранение или образование в 2013 году. Сейчас практически не осталось энтузиастов-одиночек, взламывающих сайты просто для самоутверждения, чтобы доказать себе, что они это могут. Теперь преступления в интернете — настоящий бизнес, живущий по вполне рыночным законам спроса и предложения. О том, как защитить тайну личной жизни и свои сбережения — в интервью с генеральным директором российского представительства компании ESET****Денисом МАТЕЕВЫМ***.

— Думаю, вам часто задают этот вопрос — какой у вас антивирус?

— Конечно ESET NOD32. Хотя какое-то время назад я антивирусами не пользовался вовсе.

— То есть вы патриот.

— Отчасти да. Однако, на мой взгляд, наш антивирус действительно лучше — быстрее, легче, незаметнее, надежнее.

— А можете в двух словах объяснить, зачем антивирус вообще нужен?

— В двух словах? Бороться с вирусами. Если чуть подробнее, то он защищает ваш компьютер от всех вредоносных программ (вирусы составляют лишь малую часть от них, около 17%), а также от ряда других киберугроз, которыми полон интернет.

— Кому вообще нужен мой компьютер? Я не миллионер, не известный артист, что толку преступникам от моей переписки?

— Все имеет свою цену, даже личная переписка — в ней могут оказаться секреты, за сохранение которых вы будете готовы заплатить похитителю немалые деньги. Интернет-мошенники не гнушаются шантажом. А если в вашей почте найдут, скажем, скан паспорта, отправленный в кадровый отдел при устройстве на работу, или не предназначенные для посторонних глаз фото?

Можно пострадать и от блокеров — так называются программы, которые блокируют доступ к компьютеру, требуя за разблокировку перевести определенную сумму денег (якобы код разблокировки будет написан на чеке оплаты). Можно невольно превратить свой компьютер в источник спама или вредоносных программ для всех контактов. Кроме того, вас могут просто-напросто ограбить — узнав данные, необходимые для совершения онлайн-платежей, с вашего счета могут похитить все деньги.

А можно пасть случайной жертвой — выгоды вы преступникам не принесете, а вот сами пострадаете, в том числе и финансово. Если компьютер выйдет из строя, не справившись с вредоносными программами, то вы потеряете и свои статьи, и фотографии, и сохраненные логины-пароли ко всем ресурсам, да еще будете вынуждены покупать новый ПК, или, как минимум, переустанавливать систему.

— Ну вот, скажем, я – обычный пользователь ПК. Пишу тексты, сижу во Вконтакте, иногда играю в игры. Как я могу заразиться?

— Способов невероятно много. Представьте — присылает вам красивая девушка во Вконтакте или Одноклассниках сообщение: «Привет! Хочу с тобой познакомиться! Больше моих фоток тут». И короткая ссылка, ведущая неизвестно куда. Кликнув по этой ссылке, вы в лучшем случае попадете на сайт с сомнительным содержанием, — но вместо этого, скорее всего, загрузите на свой ПК вредоносную программу. Подобное письмо могут прислать и на электронную почту — кто устоит перед сообщением в духе: «Поздравляем! Вы выиграли миллион! Чтобы узнать подробности, пройдите по ссылке…».

Из-за игр вы тоже рискуете заразиться. Лично я не сомневаюсь, что вы используете только лицензионные игры и программы, — но многие, к сожалению, до сих пор пользуются пиратскими сборками, которые часто содержат вредоносный код. Недаром авторы таких сборок настоятельно просят отключать антивирусы при установке.

Можно заразиться, просто посещая сайты — причем речь не только о вредоносных сайтах, специально созданных киберпреступниками, но и о легальных порталах, взломанных хакерами. Вы заходите на такой сайт, не подозревая, что он взломан, — а тем временем на ваш компьютер незаметно проникает вредоносная программа, открывает «черный ход» и загружает уже целый набор других программ, способных нанести вашему компьютеру и вашим данным колоссальный ущерб.

Наконец, вредоносные программы могут проникнуть и через «дыры» (их называют уязвимостями) в приложениях. Компании, производящие компьютерный софт, периодически выпускают наборы обновлений — наверняка вы получаете такие сообщения от Windows или пакета Microsoft Office. Эти обновления закрывают уязвимости, через которые могут пробраться вредоносные программы. А сколько подобных «дыр» еще не закрыты? И не только в продуктах Microsoft, но и во всех других программах.

— Какие киберугрозы сейчас наиболее опасны?

— Если говорить о тенденциях, то сейчас наблюдается стремительный рост мобильных угроз — смартфоны стали фактически переносными компьютерами, поэтому функции новых вредоносных программ для них во многом дублируют компьютерные угрозы.

Но наиболее распространенной угрозой, конечно, остается риск заражения компьютера. Сегодня около 35% компьютеров инфицированы различными вредоносными программами — и большинство пользователей об этом не подозревает.

А ведь можно стать жертвой не только вредоносной программы, но и собственной доверчивости.

— Каким образом?

— Существуют интернет-мошенники, которые обманным путем выуживают у людей ценную информацию и перепродают заинтересованным лицам, либо используют сами. Этих мошенников принято называть фишерами (от английского fish — «удить»).

Чтобы пользователь сам передал им нужные сведения, применяется целый арсенал уловок. К примеру, мошенники могут прислать «наживку» — письмо от имени администрации, скажем, вашего банка с просьбой перейти на сайт и ввести логин и пароль, код банковской карты и другую подобную информацию якобы для подтверждения личности (предлоги могут быть самыми разными).

Кликнув на ссылку в письме, вы попадете на сайт, похожий на подлинный сайт банка, но на самом деле им не являющийся. Этот сайт принадлежит преступникам, и вся информация, введенная вами, автоматически попадет к ним в руки. Подобным образом злоумышленники и воруют деньги со счетов.

А ведь существуют и другие уловки — в чем-чем, а в изобретательности киберпреступникам не откажешь. Например, широко распространено мошенничество, когда злоумышленники рассылают сообщения в духе «Мама, срочно скинь на счет 100 рублей, потом объясню». Многие верят.

Чтобы застраховаться от таких «удильщиков», нужен не только антивирус, способный распознать подозрительные ссылки, но и здравый смысл. Сейчас примерно каждый четвертый получатель фишинговых писем попадается на уловки киберпреступников.

— Пугающая картина.

— Действительно. Фишинг — второй по «популярности» способ обогащения, после распространения вредоносных программ. Надо помнить, что интернет — это не частное, а публичное пространство, даже если вы выходите в сеть из дома, сидя в кресле в уютных тапочках.

К примеру, заходя в автобус, мы краем сознания помним, что кошелек и паспорт лучше спрятать понадежнее, поскольку их могут вытащить. Также и в интернете — надо не терять бдительности и помнить о возможных рисках. Ну и, конечно, использовать хороший антивирус.

— А как вы относитесь к бесплатным антивирусам? Это ведь вполне легальные, не пиратские программы — чем не вариант?

— Полностью согласен. Использовать бесплатный антивирус — лучше, чем не иметь его вообще. Однако о реальной защите в этом случае говорить сложно. Каждый день в мире появляются десятки тысяч новых вредоносных программ, и разработчикам бесплатных антивирусов может просто не хватать ресурсов на своевременное обновление систем защиты и поддержку необходимых сервисов.

А в ESET ресурсы идут на разработку новых и улучшение существующих технологий для максимальной защиты пользователей (поэтому в технологическом плане именно продукты ESET часто становились первопроходцами). Также мы тратим большие средства на регулярное обновление вирусных баз, на возможность оперативно реагировать на угрозы, на организацию квалифицированной техподдержки, работающей в режиме 24/7.

— Трудно представить, что руководитель представительства ESET не будет расхваливать антивирусы ESET…

— А не обязательно верить мне на слово — во-первых, скорость и качество работы наших продуктов подтверждены независимыми исследованиями, а во-вторых, вы можете просто зайти на наш сайт и бесплатно скачать пробную версию программы, она действует месяц. Хотя сейчас у нас проходит много акций, по которым можно получить бесплатные антивирусы ESET и на три месяца, и на полгода, и даже на год.

В общем, просто скачайте и убедитесь в преимуществах ESET. Наш антивирус не тормозит, не выдает назойливых сообщений, не обнаруживает ложные угрозы, работает тихо и незаметно — и при этом защищает компьютер надежно, как в сейфе.

Да и его стоимость также вполне конкурентоспособна — базовую защиту можно приобрести по цене от 730 рублей.

— Многих пользователей перетянули на свою сторону? Какие вообще успехи в России?

— Мы не сторонники корпоративных войн — просто стараемся хорошо делать свое дело. Возможно, поэтому все больше людей выбирают наши продукты — тот факт, что 90% наших пользователей рекомендуют решения ESET своим друзьям и знакомым, полагаю, говорит за себя.

Про успехи могу сказать, что Россия недаром является для ESET стратегически важным регионом — многие продукты выходят в России даже раньше мирового релиза. И нам еще есть, куда расти — к 2014 году число отечественных интернет-пользователей может достигнуть 80 миллионов — и каждому из них понадобится защита от онлайн-угроз.
Источник: <http://omsk.mk.ru/article/2013/03/20/828513-kiberprestupnost-ochen-dohodnyiy-biznes.html>