Угрозы домашним ПК

— Как вы считаете, что представляет самую большую угрозу домашним ПК?
— Прокладка между стулом и компьютером! Наибольший враг домашнего ПК сам пользователь!
(Из фольклора службы поддержки)

Владимир Безмалый

Сейчас компьютеры прочно заняли место в наших домах. Мечта компании Microsoft о том, что компьютером сможет управлять каждая домохозяйка, стала реальностью. Также резко выросло число всевозможных устройств, находящихся на руках у населения.

По данным «Лаборатории Касперского», в среднем в России:

- На одну семью приходится по 3,6 различных устройства.
- Почти 67% семей имеют дома ПК.
- В 15,5% семей есть два и более ноутбуков.
- 23,8% семей имеют дома планшеты.
- 16,3% — домашний ПК, ноутбук, смартфон, планшет.

В то же время рост числа вредоносных программ за 2011 г. составил:

- Для Windows — 80%.
- Для Mac OS — 35%.

В настоящее время ежедневно(!) специалисты лаборатории фиксируют по 125 тыс. образцов вредоносного ПО по сравнению с 70 тыс. годом ранее.

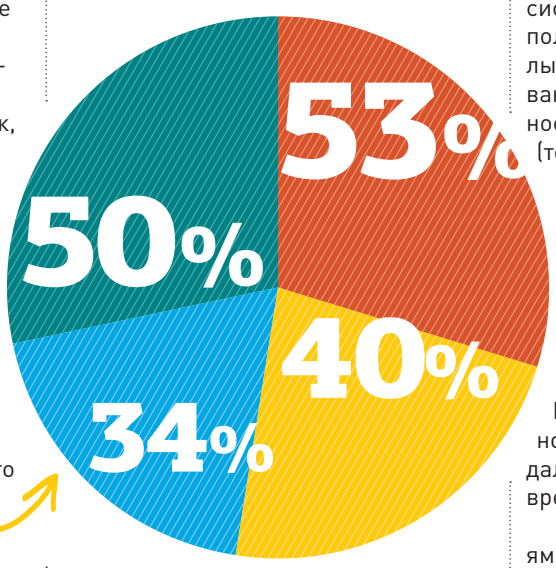
В то же время стоит отметить, что пользователи не готовы защищать себя, свои цифровые данные.

Показатели по миру внушают обоснованную тревогу: пользователи, защищающие данные с помощью примитивных, легко подбираемых паролей вроде 123456, Password и т.п., составляют 34%. Не могут распознать фишинговое сообщение 50% пользователей, сталкивались с вирусным заражением ПК или ноутбука — 53% их владельцев, а пожаловались на утечку персональных данных — 40%.

Отношение пользователей к своей безопасности

Чаще всего пользователь, покупающий ПК для дома, хочет, чтобы на нем не было предустановленной ОС (мол, зачем мне она — сосед потом поставит любую, у него есть). И сэкономив на этом весьма незначительную сумму, он остается один на один со своими проблемами в виде ворованной ОС.

Кстати, по данным специалистов компании Group-IB, каждый четвертый (25%) контрафактный дистрибутив Windows был инфицирован вредоносным ПО, а 29% нелицензионных копий платформы, доступных для скачивания в файлообменных сетях, и вовсе оказались неработоспособными. В 12,5% случаях пиратские сборки ОС включали программы для хищения паролей и личных данных пользователя и почти в каждой из них (94%) был представлен инструментарий для обхода активации Windows, потенциально негативно влияющий на стабильность работы ОС.



- Пользователи, защищающие данные с помощью примитивных, легко подбираемых паролей: 123456, Password и т. п.
- Не могут распознать фишинговое сообщение
- Сталкивались с вирусным заражением своего ПК или ноутбука
- Пожаловались на утечку персональных данных

Исследованию подверглись нелицензионные копии операционной системы, доступные российским пользователям через основные каналы распространения: в неавторизованных точках продаж на физических носителях (DVD, CD) и в Интернете (торренты и файлообменники).

Особое внимание исследователи обращают на следующее обстоятельство: отсутствие явных угроз при предварительной проверке дистрибутива антивирусом не гарантирует, что после установки в нем не окажется вредоносных программ, не обнаруженных ранее. В то же время проверка установленной ОС антивирусными средствами далеко не всегда выявляет наличие вредоносного или нежелательного ПО.

Согласно недавним исследованиям Microsoft, примерно 20% из 3229 проверенных торговых точек в 94 городах России в том или ином виде предлагают покупателям нелицензионное ПО, а 11% занимаются инсталляцией оного непосредственно в магазине. Для сравнения: несколькими месяцами ранее в торговлю пиратским ПО было вовлечено более четверти (27%) российских магазинов. В целом уровень компьютерного пиратства в России остается значитель-

но выше среднемирового: 67% против 43% соответственно.

На мой взгляд, основная угроза для пользователей — они сами! Почему?

Да потому, что пользователи не предпринимают никаких мер по обеспечению собственной же безопасности, несмотря на неоднократные призывы устанавливать лицензионное ПО, регулярно обновлять ОС и приложения, актуализировать антивирусы, использовать устойчивые пароли и не разглашать свои персональные данные в социальных сетях.

Обратимся к результатам исследования «Лаборатории Касперского».

Наиболее актуальной проблемой для пользователей остается нежелательная корреспонденция — с ней, независимо от используемого устройства, сталкивались 69% опрошенных. Причем она включает в себя как условно безопасный спам, так и письма или сообщения с подозрительными ссылками, которые способны заразить устройства. От действий вредоносного ПО пострадали 56% пользователей ПК, а 13% владельцев планшетов и 10% обладателей смартфонов также оказывались в ситуации, когда их устройство не могло нормально работать из-за вредоносной программы.

От действий различных троянцев-вымогателей пострадали 29% опрошенных, в основном пользователей ПК. Еще 35% сталкивались со всплывающими окнами, сигнализирующими о мнимом заражении устройства, и рекомендациями установить фальшивый антивирус. Еще одна заметная угроза — утечка персональных данных, ее жертвами в разное время были 44% опрошенных. Причем разрыв между пользователями ПК и владельцами мобильных устройств здесь не так заметен, как, например, в случае со всплывающими окнами. Так, с доступом посторонних лиц к аккаунту в социальной сети или электронной почте сталкивались 16% пользователей ПК и 10% владельцев планшетов.

Около трети опрошенных получали фишинговые сообщения. Причем 11% потенциальных жертв киберпреступников пользовались смартфонами, а 14% — планшетами, что опять же свидетельствует о том, что владельцы мобильных устройств больше не находятся в безопасности. С такой крайне важной проблемой, как утечка финансовой информации, пришлось иметь дело 21% опрошенных. Интересно, что заметная доля пользователей ПК (13%), владельцев планшетов (8%) и смартфонов (6%) признаются, что вводили персональные данные на вебсайтах, выглядящих как минимум подозрительно.

Несмотря на то что стоимость современных пакетов защиты (класса Internet Security) сравнительно невелика, бесплатные антивирусные решения все еще очень популярны. По данным исследования, ими пользуются почти две трети потребителей по всем миру. И хотя большинство бесплатных антивирусов обеспечивают только базовую защиту компьютера и не способны блокировать наиболее опасные угрозы, значительное число пользователей уверены, что их достаточно для обеспечения безопасности компьютера.

Многие современные компьютеры и ноутбуки продаются с предустановленной пробной версией антивирусного ПО, чаще всего класса Internet Security. Подобные программы применяли около 60% опрошенных. Однако после окончания испытательного периода 30% пользователей устанавливают антивирусный продукт другого разработчика и лишь 13% покупают лицензию. Интересно, что в среднем 2% пользователей не предпринимают никаких действий после окончания испытательного периода, т.е. фактически оставляют компьютер без защиты.

Основным средством защиты пользовательских аккаунтов, например электронной почты, является пароль. И тут сами пользователи порой проявляют потрясающую беспечность: 34% опрошенных используют очевидные и простые пароли. Некоторые из них можно найти в свободном доступе в социальных сетях, например, дату рождения (выбирают 17%) или кличку домашнего животного (9%). Другие — набор цифр «123456» и вариации (8%) или «Password» (5%) — очень легко подобрать. Слабые пароли представляют собой один из самых заметных пробелов в безопасности пользовательских данных.

Вместе с тем стоит подчеркнуть, что многие не обновляют свои ОС и прикладное ПО.

Исследование, проведенное специалистами компаний Skype, Norton, Symantec и TomTom в рамках программы International Technology Upgrade Week, показало, что почти половина пользователей ПК не проводят своевременного обновления программного обеспечения.

Большинство из них ссылаются на нехватку времени, однако некоторые респонденты заявили, что не понимают, каким образом устанавливаются обновления. Более того, почти четверть опрошенных не знают, зачем они вообще нужны.

Опрос был проведен среди 350 тыс. пользователей в Великобритании, США и Германии. Причем 40% из тех, кто принял участие в опросе, заявили, что не обновляют свое ПО, даже когда увидят соответствующее уведомление.

Почти 60% опрошенных отметили, что просматривают уведомление о наличии обновлений, однако чаще всего откладывают установку, а более 50%

К чему может привести любовь к халяве?

(Недавний случай)

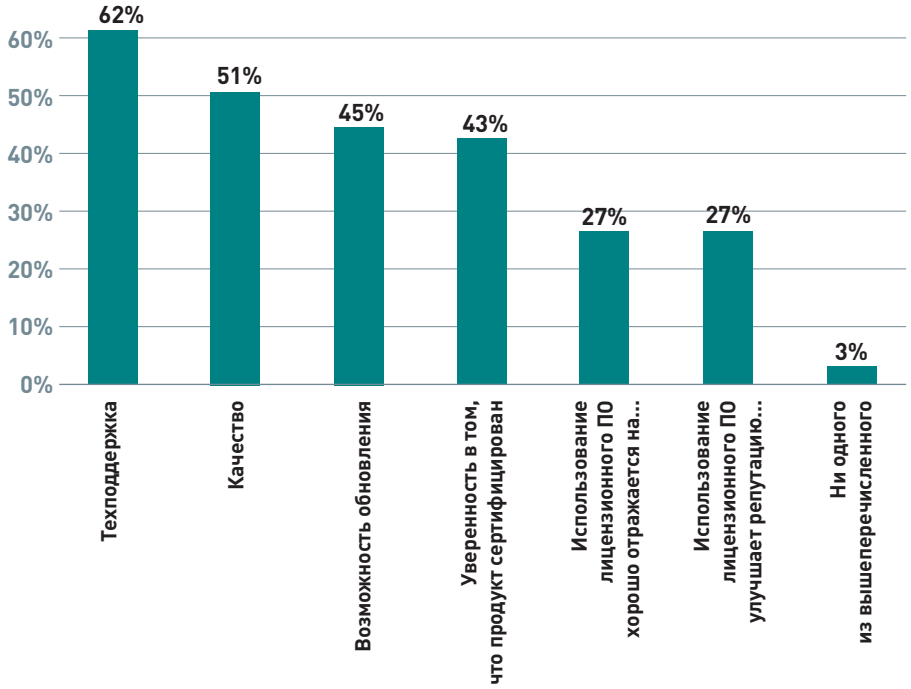
Компьютерные злоумышленники создали 10 интернет-ресурсов и, выдавая их за официальные сайты компании-разработчика, предлагали пользователям загрузить якобы лицензионную программу «Навител Навигатор». Однако было установлено, что она изменена таким образом, что после скачивания могла работать без лицензии и сертификата правообладателя. За год существования ресурса модифицированное ПО было скопировано пользователями Интернета более 38 тыс. раз.

После установки программы пользователю следовало отправить SMS-сообщение на короткий номер, чтобы получить код активации. Это стоило 300 руб., в то время как цена легально распространяемого продукта — 2400 руб. Таким образом, ущерб, причиненный правообладателю, составил свыше 90 млн. руб.

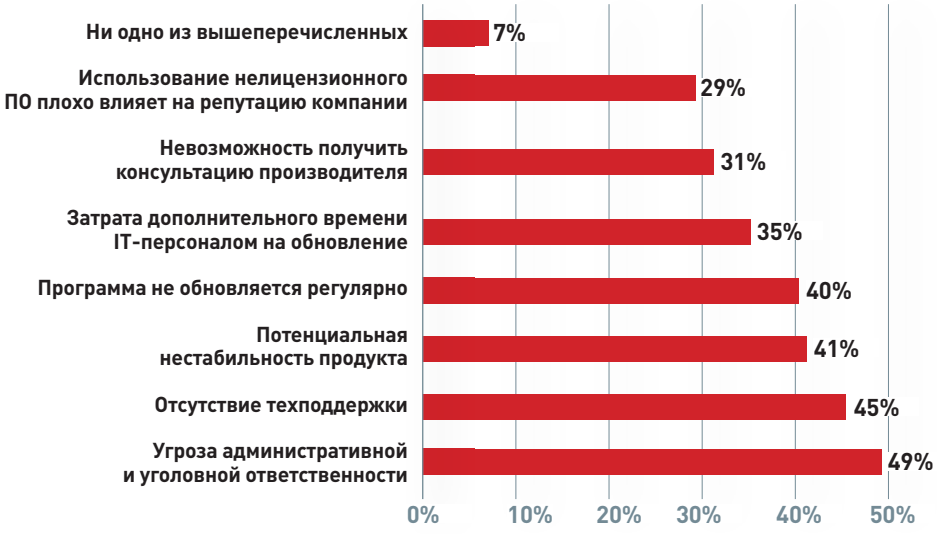
Помимо того, что скачанная нелицензионная программа работала некорректно, при ее установке на смартфоны она выполняла вредоносные функции, то есть скрытно от пользователя отправляла SMS на короткие номера, из-за чего происходило регулярное несанкционированное списание денежных средств со счета.

Таким образом, люди, решившие сэкономить, на самом деле сами добровольно отдавали злоумышленникам деньги.

Преимущества лицензионного защитного ПО с точки зрения российских малых и средних компаний



Недостатки нелицензионного защищенного ПО с точки зрения российских малых и средних компаний



использование социальных сетей. Почти половина опрошенных назвала их главным источником угроз. На втором месте прочно обосновались сменные носители.

Так, 60% малых и средних компаний в России запрещают своим сотрудникам доступ к социальным сетям, 69% — к онлайн-играм, а 52% — к P2P-сетям для обмена файлами (например, BitTorrent, eDonkey).

Так почему же наблюдается такой разброс в цифрах по Европе и США и по России в целом?

Прежде всего потому, что у нас к сектору малых предприятий традиционно относятся те, на которых работают от одного до десяти ПК. Как правило, обеспечением информационной безопасности там занимается системный администратор, к тому же зачастую являющийся приходящим раз в неделю работником. Естественно, в таком случае говорить о качественном обеспечении требований ИБ просто не приходится. На это нет ни времени, ни денег, ни желания. Кроме того, руководство фирмы обычно просто не задумывается об этом. Чаще всего можно услышать: «Да что у нас воровать? Вот украдут, тогда и думать будем, а пока на насущные проблемы денег нет!»

С одной стороны, такой подход, безусловно, имеет место, а с другой — вполне понятно, почему думают именно так. Для того чтобы задумываться о проблеме информационной безопасности, нужно быть уверенным в том, что твой бизнес просуществует еще хотя бы лет пять. Думаю, что у большинства владельцев малых предприятий такой уверенности просто нет. Тут бы как-то с налоговой (пожарной, санитарной) службами договориться, а вы об информационной безопасности. И пока бизнес строится таким образом, у информационной безопасности будет один из самых низких приоритетов! ■