# ВЫЖИТЬ В ЦИФРОВОМ МИРЕ

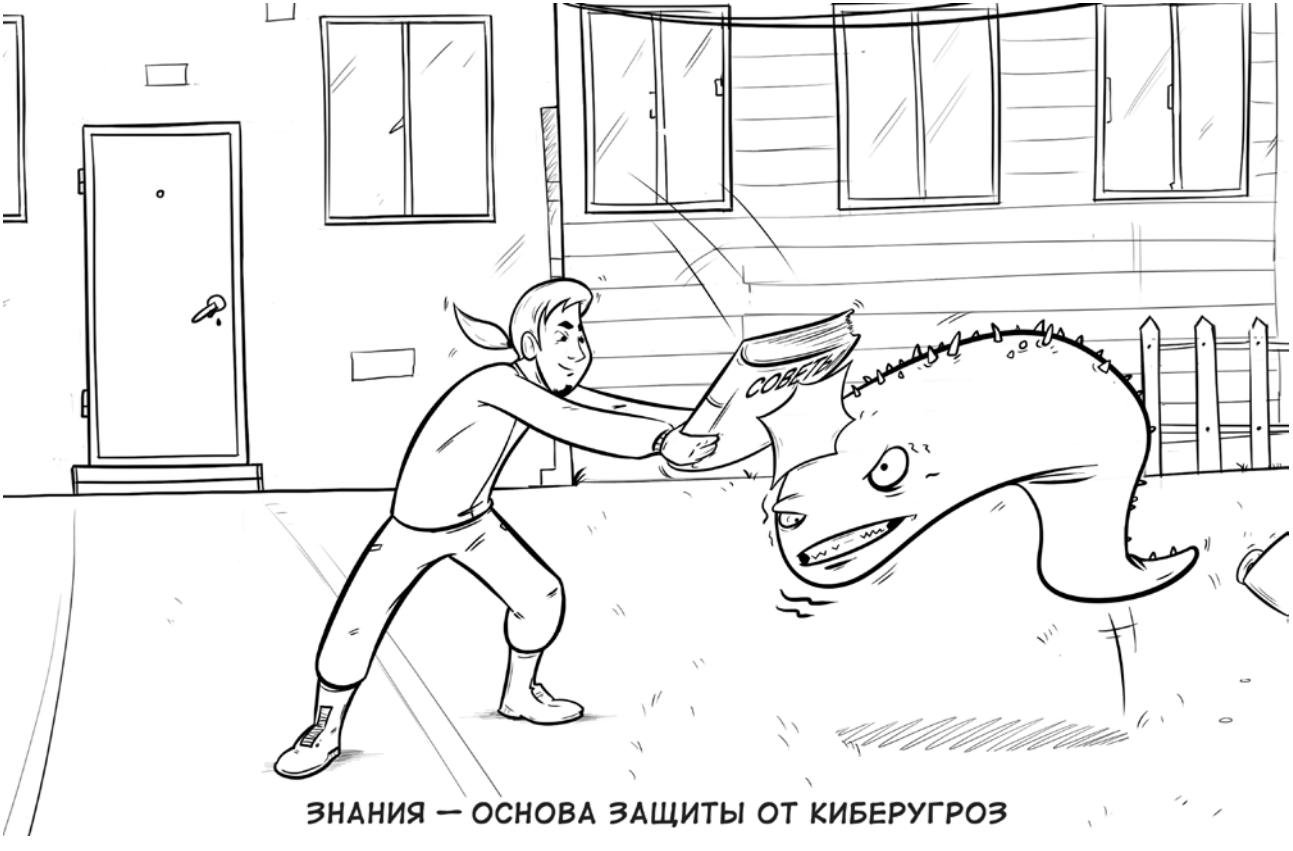
Иллюстрированные советы от «Лаборатории Касперского»

KASPERSKY lab

# ПРЕДИСЛОВИЕ

Расцвет цифрового мира оказался не совсем таким, как мы ожидали. Персональные компьютеры и мобильные устройства подарили людям доступ к знаниям и новые возможности для обмена ими; жизнь стала проще и лучше благодаря новым технологиям, в первую очередь Всемирной паутине. Но очень скоро оказалось, что у медали есть и обратная сторона: появились первые случаи кражи личной информации, цифровые вредоносные программы научились наносить реальный ущерб, а различные преступники и извращенцы стали использовать Сеть как личную игровую площадку.

Но нашлись те, кто выступил против хаоса и собрал весь свой опыт борьбы с ним, чтобы передать его следующим поколениям. Здесь мрачная часть легенды заканчивается, и начинается наша история...

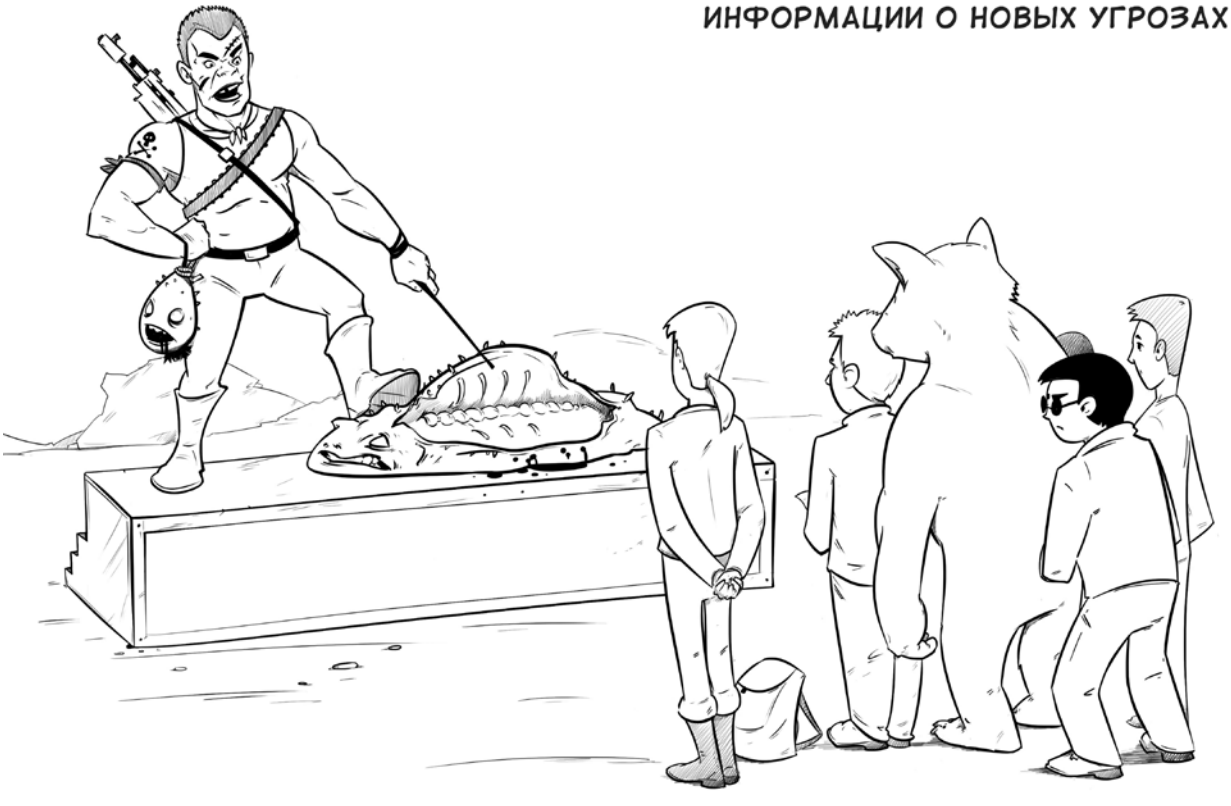



ЗНАНИЯ — ОСНОВА ЗАЩИТЫ ОТ КИБЕРУГРОЗ

# СОВЕТ 1: **ПОЛЕЗНЫЕ ЗНАНИЯ**

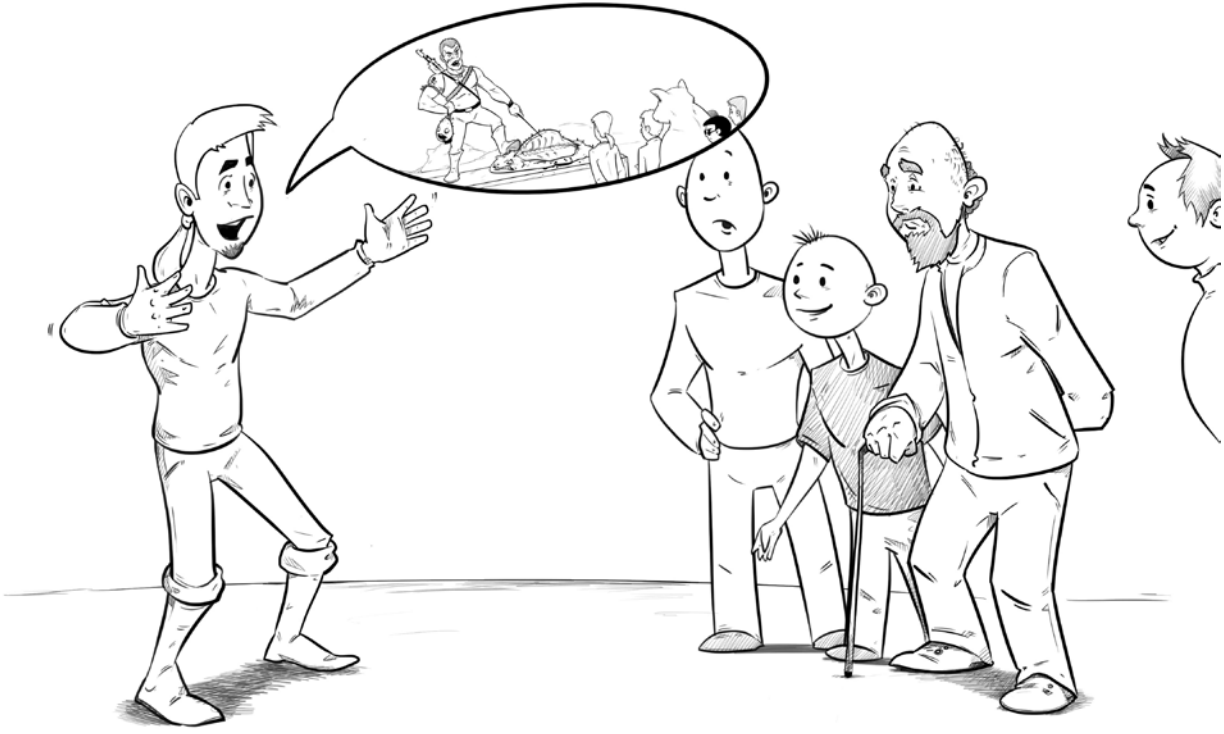
Представьте себе: вирус проникает в компьютер по телефонной сети, включает его среди ночи и дает команду на запуск ядерных ракет... Живая картинка получается? Если да, то благодарить за это надо голливудские фильмы, далекие от реальности. В жизни вредоносные программы действуют по-другому и, как правило, атакуют иные цели. Вирусы используют как уязвимые места компьютерных систем, так и незнание их пользователями основ информационной безопасности. Звучит невероятно, но если хакер захочет заразить чей-нибудь компьютер, ему не нужно будет писать сотни строчек абракадабры под тревожную музыку, достаточно лишь послать пользователю электронное письмо с зараженным вложением. Если текст письма будет достаточно убедительным, жертва сама запустит вложенную вредоносную программу. Потому победа честных людей в соревновании с киберпреступниками напрямую зависит от их осведомленности об угрозах.

БЛОГИ ВЕДУЩИХ АНТИВИРУСНЫХ КОМПАНИЙ — ОТЛИЧНЫЙ ИСТОЧНИК ИНФОРМАЦИИ О НОВЫХ УГРОЗАХ



# СОВЕТ 2: **ИСТОЧНИКИ ИНФОРМАЦИИ**

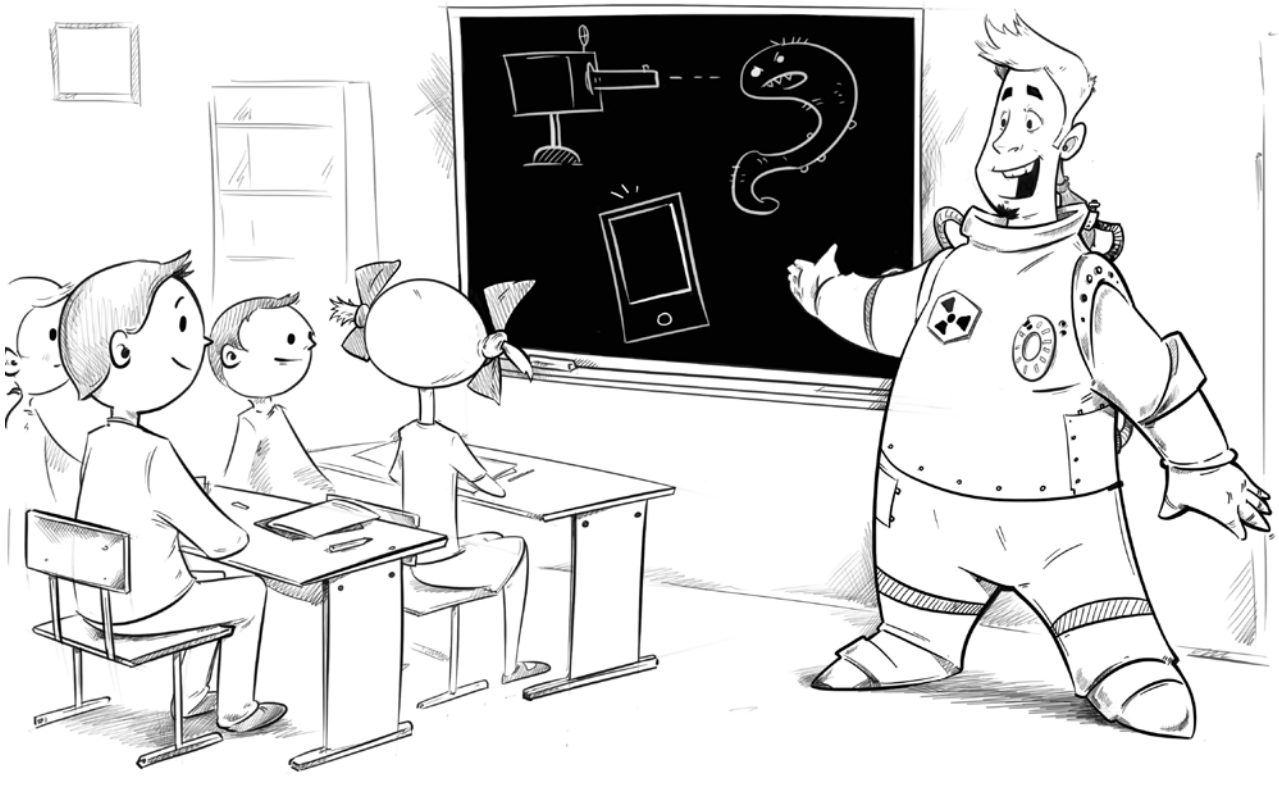
Предупрежден — значит вооружен, и это особенно верно для информационных угроз. В войне между угрозами и защитой от них побеждает даже не тот, кто лучше оснащен, а тот, кто больше знает о противнике. В блогах антивирусных компаний всегда можно найти сведения о вирусах, приемах злоумышленников и уязвимостях в ПО. Оттуда же внимательный читатель узнает, как не попасться на удочку преступников и предотвратить атаку на свой компьютер.



ДЕЛИТЕСЬ ПОЛУЧЕННЫМИ ЗНАНИЯМИ С РОДНЫМИ

# СОВЕТ 3: **ЗАБОТА О БЛИЗКИХ**

Для атак на честных пользователей хитроумные хакеры изобрели фишинг, эксплойты, малвертайзинг и другие непонятные слова. Но это не самое опасное. Самое сильное оружие в арсенале киберпреступников — неосведомленность их жертв о киберугрозах. Нельзя защититься от того, о чьем существовании ты не подозреваешь, и тут на первый план выходит свободный обмен информацией между потенциальными жертвами. Не стесняйтесь рассказывать родным о новых киберугрозах во всех подробностях, помните: предупрежден — значит вооружен.



ПОДЕЛИТЕСЬ С ДЕТЬМИ ЗНАНИЯМИ О КИБЕРМИРЕ

# СОВЕТ 4: **ОБУЧЕНИЕ ДЕТЕЙ**

Даже самые современные родители склонны недооценивать скорость, с которой ребенок осваивает компьютер, гаджеты и интернет. Еще вчера он не умел говорить, а сегодня уже зарегистрирован на десятках сайтов и ведет свой канал на YouTube. И именно от вас зависит, каким кибератакам он сможет противостоять — никто другой не расскажет ребенку о соблазнах и опасностях Сети. Эти знания современному подростку становятся необходимы гораздо раньше, чем половое воспитание.

НЕ ОСТАВЛЯЙТЕ СВОЙ ПОЧТОВЫЙ АДРЕС В ПУБЛИЧНЫХ МЕСТАХ,
ЕСЛИ НЕ ХОТИТЕ СТАТЬ МИШЕНЬЮ СПАМЕРОВ

# СОВЕТ 5: **ПОЧТА БЕЗ МУСОРА**

Возможность обратиться к каждому жителю планеты с проникновенными словами и выгодным коммерческим предложением — голубая мечта некоторых работников рекламной индустрии, которая стала реальностью благодаря электронной почте. В наше время с такими людьми за руку уже не здороваются, так как поток рекламных писем (спама) превысил все разумные пределы, создавая серьезную нагрузку на интернет и психику пользователей, вынужденных каждый день очищать электронный ящик от рекламы. Чтобы не тратить время на мусор, избегайте «светить» свои адреса в общедоступных местах — уже через несколько секунд после размещения электронного адреса на публичном форуме он попадает в руки спамерам. Плоды прогресса!


ВНИМАТЕЛЬНО ИЗУЧИТЕ ОФИЦИАЛЬНОЕ ПИСЬМО,
ПРЕЖДЕ ЧЕМ СЛЕДОВАТЬ НАПИСАННОЙ В НЕМ ИНСТРУКЦИИ

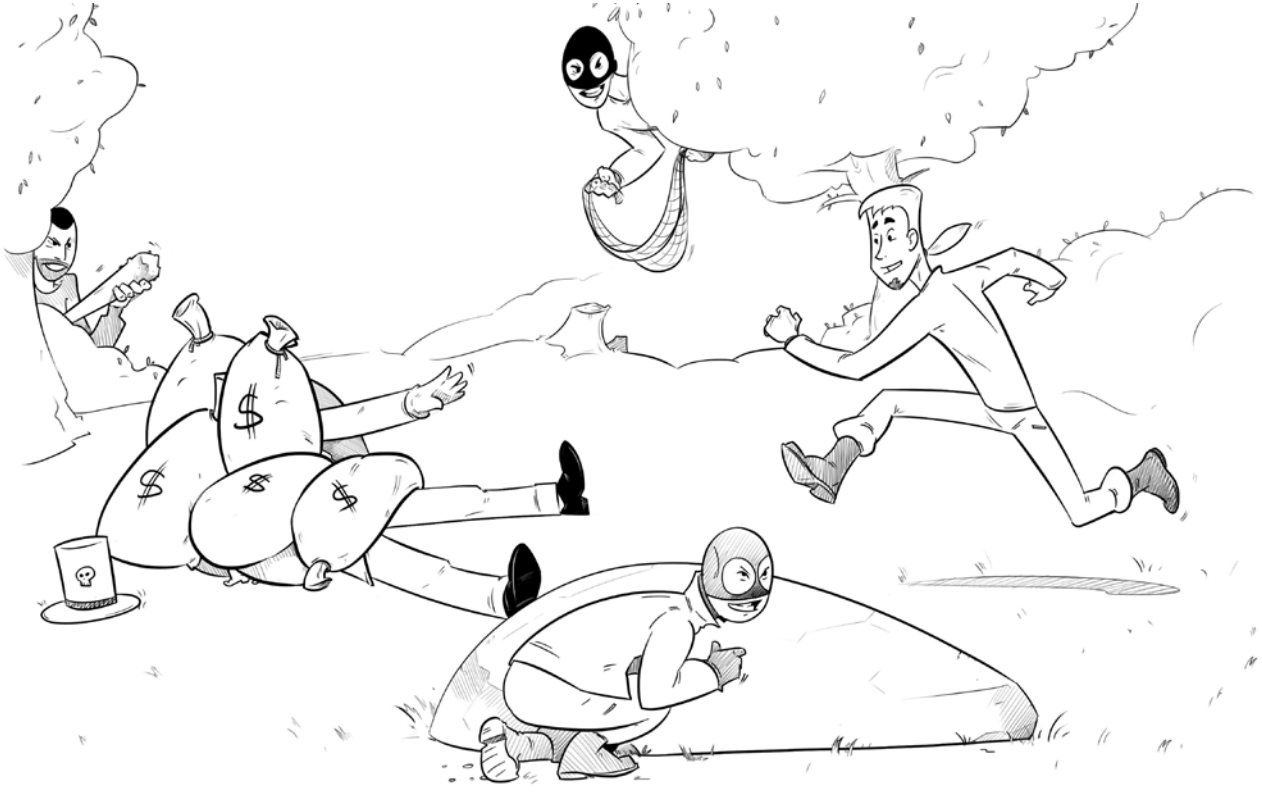
# СОВЕТ 6: **ПОДДЕЛЬНЫЕ ПИСЬМА**

Не ждали электронного письма от налоговой службы, а оно пришло? Да еще и с требованием немедленно уплатить штраф, пока дело не передали в прокуратуру, суд или расстрельную команду? Не горячитесь и не спешите кликать по ссылкам из письма или открывать приложенные документы. Сначала убедитесь, что это письмо действительно от ФНС, ведь поддельные письма от имени различных государственных служб и известных компаний — один из самых популярных способов распространения киберзаразы. Злоумышленники могут называть себя налоговиками, представителями суда или другими госслужащими, представителями социальной сети или интернет-провайдера — кем угодно, лишь бы заставить вас потерять бдительность и выполнить необходимые им действия. Потому не поленитесь проверить подлинность сообщения по другим каналам связи, например позвоните в местную налоговую по телефону.


НЕ ОТКРЫВАЙТЕ СОМНИТЕЛЬНЫЕ ВЛОЖЕНИЯ

# СОВЕТ 7: **СКРЫТАЯ УГРОЗА**

Вы любите сюрпризы? Хорошая новость — в интернете полно людей, которые любят их делать. Есть и другая новость, похуже: эти сюрпризы вам не понравятся, поскольку в их создании приняли участие злоумышленники и вредоносное программное обеспечение. Например, если вам пришло письмо со ссылкой на «крутое видео, обхохочешься!» или вложенным архивом с «фотками с той тусовки», задумайтесь: кто вам его прислал и зачем? Весьма вероятно, что отправитель письма вам незнаком, а в архиве вместо желанных фотографий сидит троянец. Поэтому не открывайте такие вложения, даже если вы очень, очень любите сюрпризы.



НЕ ВЕРЬТЕ НЕСЧАСТНЫМ «НИГЕРИЙСКИМ» МИЛЛИОНЕРАМ

# СОВЕТ 8: **ФАЛЬШИВЫЕ БОГАЧИ**

Если киберархеологи далекого будущего возьмутся разбираться в триллионах электронных писем нашей эпохи, их наверняка изумит количество миллионеров, проживавших в Нигерии. Возможно, эта страна даже войдет в учебники как волшебный край, где жили сказочно богатые, но поголовно несчастные люди. В наше время в такие сказки верить не стоит: даже если в этой небогатой, скажем прямо, стране, отыщется миллионер, вряд ли он станет взывать о помощи к незнакомому человеку из далекой России, да еще и по электронной почте. На самом деле письма от имени нигерийских мошенников, африканских принцев и других богатых, но несчастных персонажей рассылают мошенники, рассчитывающие поживиться за счет людской жадности. Желающие разделить с «миллионером» его богатство платят «за оформление денежного перевода», оплачивают «налог на наследство» или «гонорар юриста» и тем самым кормят голодного, но хитрого обитателя далекой страны (необязательно Нигерии) и всех его сообщников.

СПАМ-РАССЫЛКА — ПЛОХОЙ ИСТОЧНИК ПРЕДЛОЖЕНИЙ О РАБОТЕ

# СОВЕТ 9: **ОПАСНЫЙ СПАМ**

Рабовладельцы и не подозревали, что многие люди сами рады впрячься в ярмо без какой-либо платы. Все, что нужно, — обмануть их, внушив надежду на золотые горы. И самый простой способ массового набора бесплатной или крайне дешевой рабочей силы — обычный спам. Главное, придумать заголовок поярче и обещания попривлекательнее. Вы умны и никогда не попадетесь на заманчивое предложение заработка в интернете? Что ж, эти «бизнесмены» обойдутся и без вас, среди миллионов получателей рекламных посланий несколько сотен добровольцев обязательно найдется.

КРАЖА ЛИЧНЫХ ДАННЫХ ПРИВОДИТ К КРАЙНЕ НЕПРИЯТНЫМ ПОСЛЕДСТВИЯМ

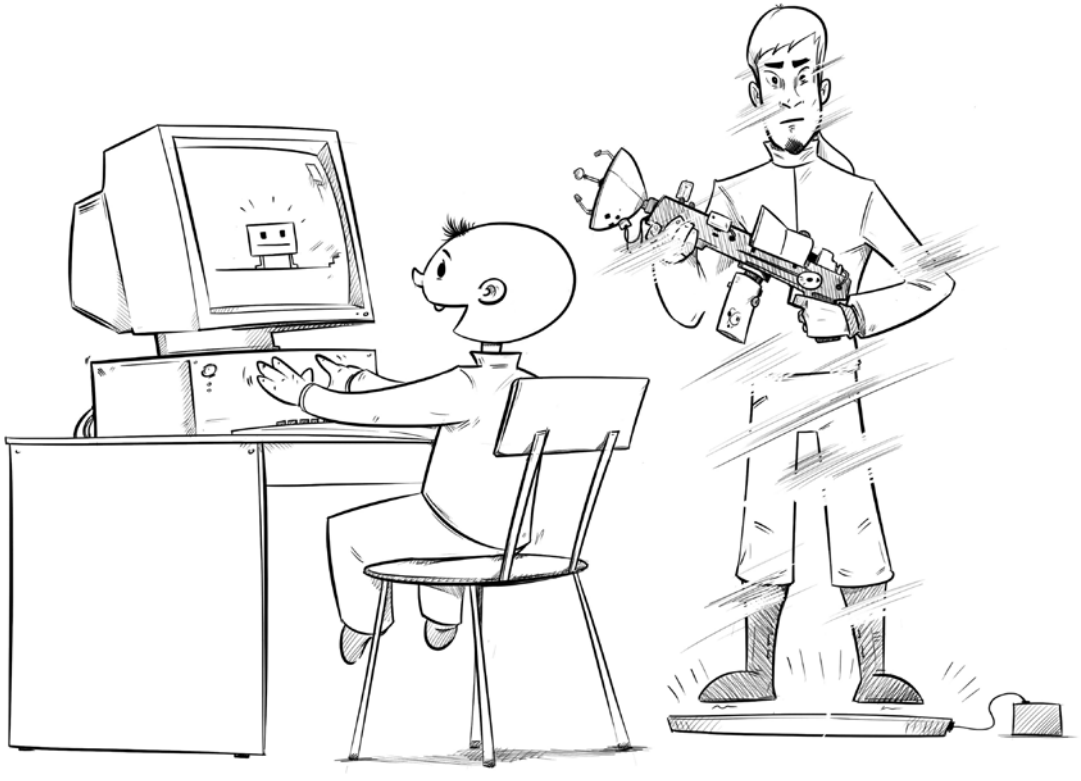
# СОВЕТ 10: **ЗАЩИТА ЛИЧНОСТИ**

Все люди рождены разными, но в интернете пользователь Вася отличается от пользователя Пети в основном уникальным сочетанием имени и пароля, которые, как и любые другие данные, можно украсть или подделать. И если Васе понадобилось выдать в Сети себя за Петю, ему достаточно пройти процедуру «восстановления пароля», для которой нужно лишь вызнать о Пете несколько деталей, что может быть совсем нетрудно — зачастую достаточно изучить открытый профиль Пети в социальной сети, где уже написано много интересного. Например, можно найти дату рождения супруги или кличку любимой собаки Пети, которые могут использоваться в качестве ответов на контрольный вопрос при регистрации ящика электронной почты. А завладев почтой Пети, Вася сможет получить доступ ко всем сервисам, где Петя указал этот почтовый адрес в качестве адреса регистрации, а также разослать его друзьям интересные письма. Мораль проста: персональные данные имеют высокую ценность, не стоит ими бездумно разбрасываться.


УЧЕТНАЯ ЗАПИСЬ РОДИТЕЛЕЙ — ПРОПУСК В МИР ВЗРОСЛЫХ

# СОВЕТ 11: **ИНТЕРНЕТ ДЛЯ ДЕТЕЙ**

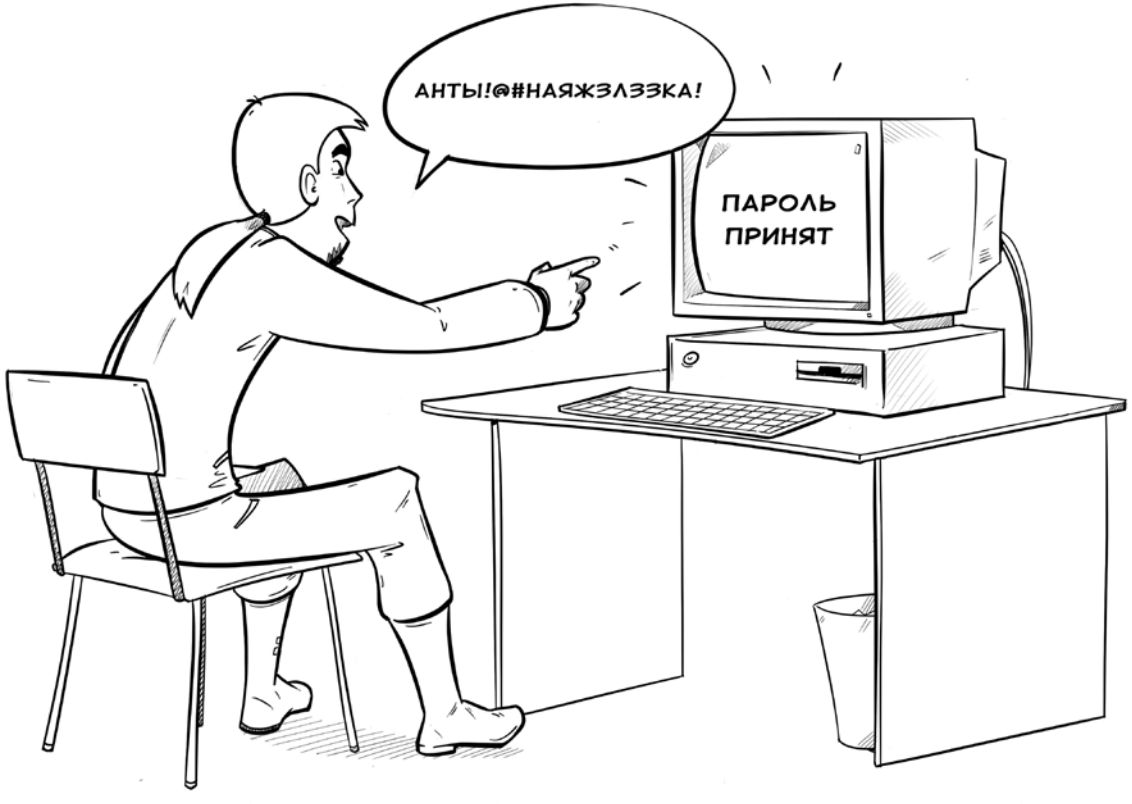
В большинстве случаев программы родительского контроля отлично работают, ограждая ребенка от вредной информации и нежелательного общения в интернете. Однако они не помогут, если дитя узнало пароль от вашей учетной записи и набралось достаточно храбрости, чтобы зайти в Сеть с вашими, взрослыми, правами доступа. Ребенок не может сойти за взрослого в реальной жизни, но в кибермире все становится проще, поскольку реальное фото у пользователя требуют редко, а документы — еще реже. Помните, что чем строже вы запрещаете что-либо ребенку, тем сильнее ему этого хочется. Да и в любом случае, не стоит хранить пароль в доступном месте.



ЗАЩИТИТЕ РЕБЕНКА ПРИ ПОМОЩИ РОДИТЕЛЬСКОГО КОНТРОЛЯ

# СОВЕТ 12: **ЗАЩИТА РЕБЕНКА**

Когда ваша дочь-третьеклассница начнет выражаться как сапожник, да еще и проявит поразительную осведомленность в вопросах взаимоотношений полов, не спешите ругать ее одноклассников или невоздержанных на язык соседей. Источник зла, скорее всего, не во дворе и не в школе, а в компьютере ребенка. Многие родители дают любимому чаду доступ в интернет ради его развития и успехов в учебе, не озаботившись фильтрацией содержимого Сети — а ведь немалая ее часть совсем не предназначена для детей! Есть три варианта: отнять компьютер, постоянно стоять за спиной ребенка, внимательно следя за тем, что он делает за компьютером, или же воспользоваться программами родительского контроля. Выбирайте на свой вкус.




ИСПОЛЬЗУЙТЕ ТВОРЧЕСКИЙ ПОДХОД К СОЗДАНИЮ ПАРОЛЕЙ...

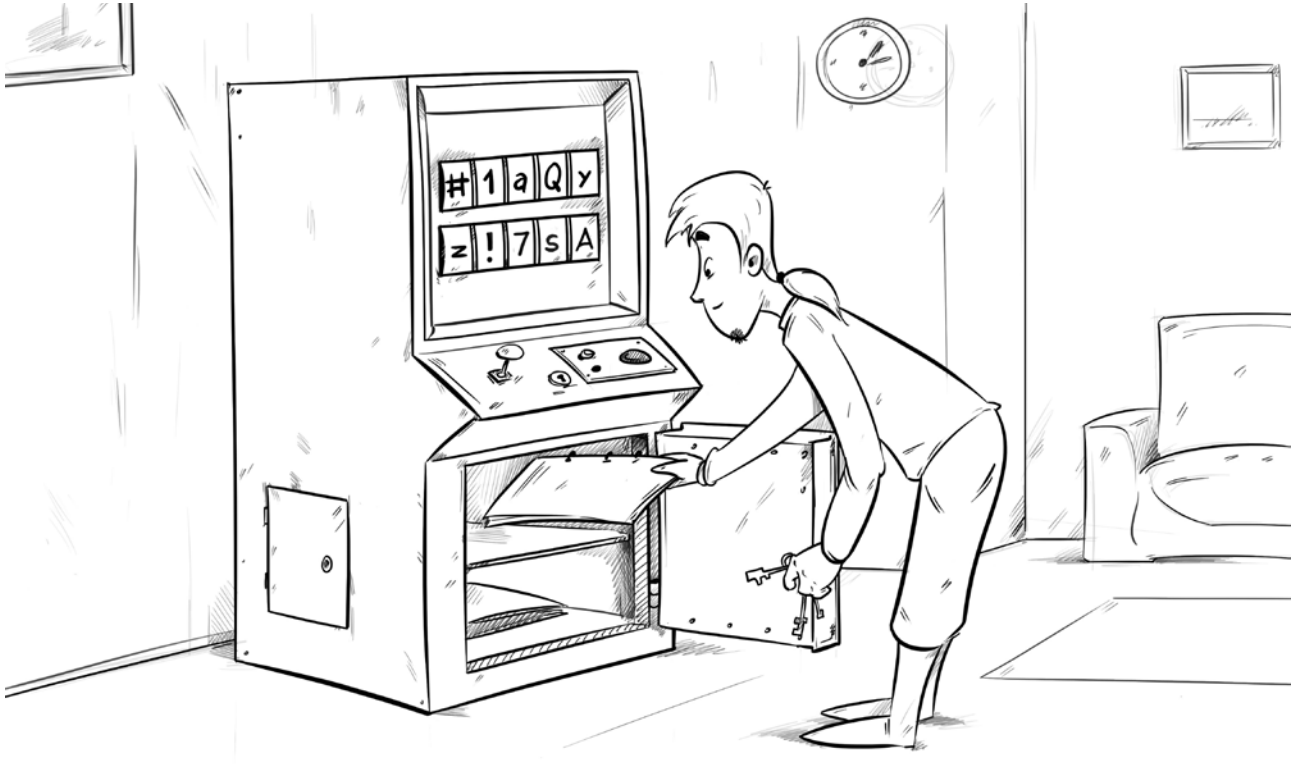
# СОВЕТ 13: **СЛОЖНЫЙ ПАРОЛЬ**

Хакеры начинают подбор пароля с проверки по специальным словарям, в которых содержатся миллионы паролей, когда-то где-то использованных. Так что все пароли, которые сходу придут вам в голову, скорее всего, в этих словарях уже есть — среди миллионов людей наверняка нашлись ваши собратья по складу ума. Но в любом случае не следует использовать в качестве пароля распространенные слова, строчки из песен или названия фильмов, кличку своего кота, дату рождения и другую информацию, которую легко найти в социальных сетях или угадать.


...И ДЕЛАЙТЕ ИХ ПО-НАСТОЯЩЕМУ СЛОЖНЫМИ
ДОСТУП
ЗАПРЕЩЕН

# СОВЕТ 14: **НАДЕЖНЫЙ ПАРОЛЬ**

Простой способ создать сложный пароль — ассоциации. Выберите слово-сочетание, ассоциирующееся с сервисом или сайтом, для которого нужен пароль, наберите его на латинице, разбавьте несколькими цифрами и спец-символами, и в результате получите достаточно длинный и надежный пароль. Главное, такой пароль нетрудно запомнить, ведь кажущееся на первый взгляд бессмысленным сочетание букв, цифр и символов будет иметь смысл для вас.




ИСПОЛЬЗУЙТЕ МЕНЕДЖЕР ДЛЯ СОЗДАНИЯ И ХРАНЕНИЯ ПАРОЛЕЙ

# СОВЕТ 15: **ХРАНЕНИЕ ПАРОЛЕЙ**

Чем сложнее пароль, тем сложнее его подобрать. Чем проще пароль, тем проще его запомнить. Получается, пароль должен быть и сложным, и простым одновременно — парадокс, решить который не каждому под силу. Если совет с ассоциациями вам не подходит, попробуйте специальную программу-менеджер паролей. Она создаст для вас сложные, уникальные (!) пароли для онлайн-сервисов, социальных сетей, приложений и пр., а затем сохранит их в своей зашифрованной базе. И вам останется только придумать один, самый главный пароль от менеджера паролей. Помните: он должен быть таким сложным, чтобы его нельзя было подобрать, и таким простым, чтобы его можно было запомнить!


КОПИЮ ЦЕННЫХ ДАННЫХ МОЖНО РАЗМЕСТИТЬ В УДАЛЕННОМ ХРАНИЛИЩЕ...

# СОВЕТ 16: **РЕЗЕРВНОЕ КОПИРОВАНИЕ**

Компьютеры тоже смертны, и более того, внезапно смертны. Зачастую потерять «железо», даже самое современное, далеко не так обидно, как утратить архив семейных фотографий, почти доделанный дипломный проект или, скажем, собиравшееся годами портфолио. К счастью, все это задешево — а то и бесплатно — можно разместить в катастрофоустойчивом центре обработки данных, принадлежащем крупной компании. Самостоятельно или с помощью специального ПО можно регулярно копировать данные с компьютера или смартфона в этот центр, чтобы они были под рукой на случай аварии. Это называется облачным хранилищем, и такие хранилища сейчас весьма распространены.


...ТОГДА ВАШИ ФАЙЛЫ ПЕРЕЖИВУТ ЛЮБУЮ КАТАСТРОФУ

# СОВЕТ 17: **БЕЗОПАСНОСТЬ ДАННЫХ**

Благодаря удаленным хранилищам, даже в случае полного вымирания человеческого рода в результате какого-либо катаклизма, будущие инопланетные исследователи Земли смогут полюбоваться на интерьеры земных туалетов и лифтов, заслоненных упитанными любителями селфи, послушать песни Джастина Бибера и прочитать миллионы текстов, которые ежесекундно извергают сегодня все графоманы человечества.

ДОБАВЛЯЙТЕ В ДРУЗЬЯ ТЕХ, КОГО ЗНАЕТЕ ЛИЧНО

# СОВЕТ 18: **ПРОВЕРЕННЫЕ ЗНАКОМСТВА**

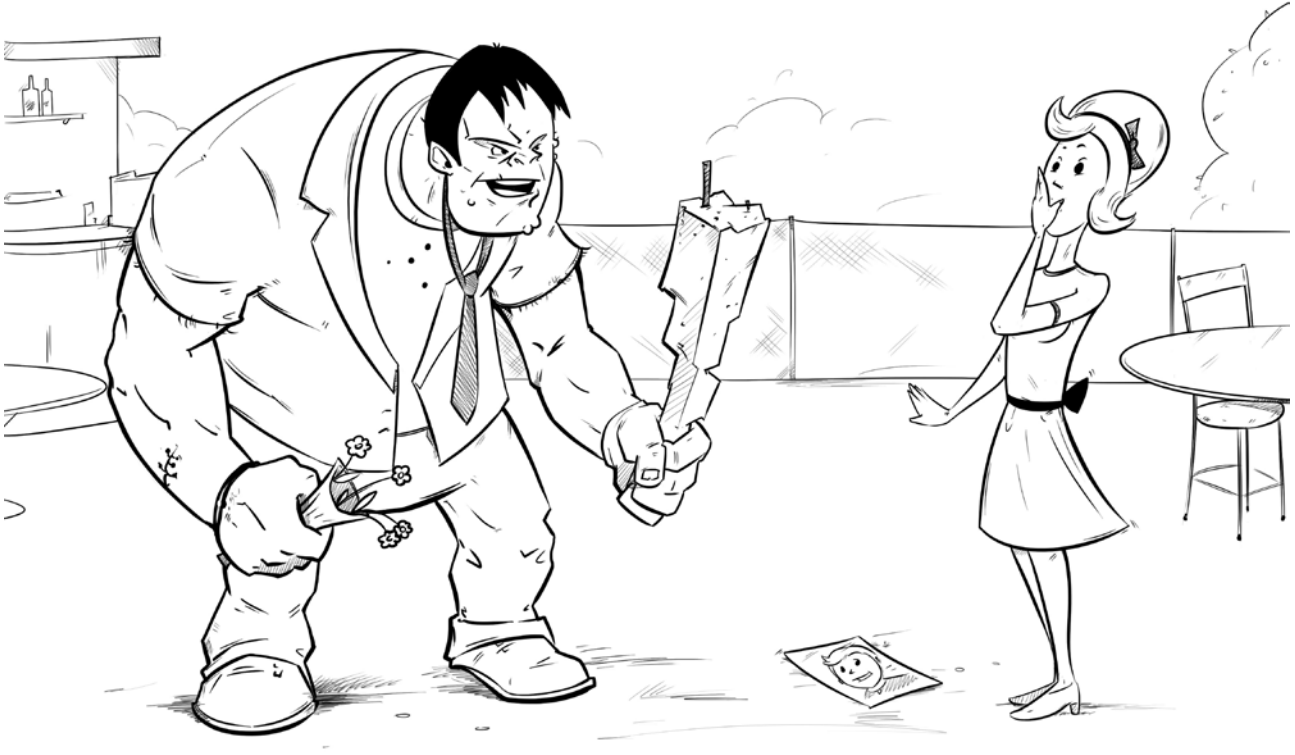
Словарное значение слов «friend» и «друг» одинаково, но в жизни не стоит принимать виртуальных френдов за друзей. Одно дело, когда у вас сетевая дружба с теми, кого вы хорошо знаете в реальной жизни, и совсем другое дело — бездумное добавление в список контактов всех, кто пожелал с вами общаться. Беспорядочные связи в реальной жизни очень часто заканчиваются тем, что излишне дружелюбный человек получает от новых «друзей» массу неприятностей, от конфликтов в семье до ограбления. Аналогично и в киберпространстве, живо интересующиеся вами незнакомцы запросто могут оказаться мошенниками, педофилами, распространителями вредоносных программ или просто спамерами.

ОПАСАЙТЕСЬ СОБЛАЗНИТЕЛЬНЫХ ИНТЕРНЕТ-КРАСАВИЦ...

# СОВЕТ 19: **РОКОВЫЕ КРАСАВИЦЫ**

Интернет-знакомства сродни уравнению со многими неизвестными. Или лучше сравнить их с «русской рулеткой»? В Сети партнер покажет вам лишь то, что хочет показать, и даже многодневная переписка не даст вам полной уверенности в личности того, кто сидит по ту сторону экрана. О мотивах поведения незнакомого человека «на той стороне» можно только гадать, и вам еще повезет, если интернет-красавица просто окажется не красавицей — обманом могут быть заявленные семейное положение, возраст и даже половая принадлежность.

...ДА И ИНТЕРНЕТ-КРАСАВЦЫ НЕ ВСЕГДА ОПРАВДЫВАЮТ ОЖИДАНИЯ



# СОВЕТ 20: **НЕЖЕЛАТЕЛЬНЫЕ СВЯЗИ**

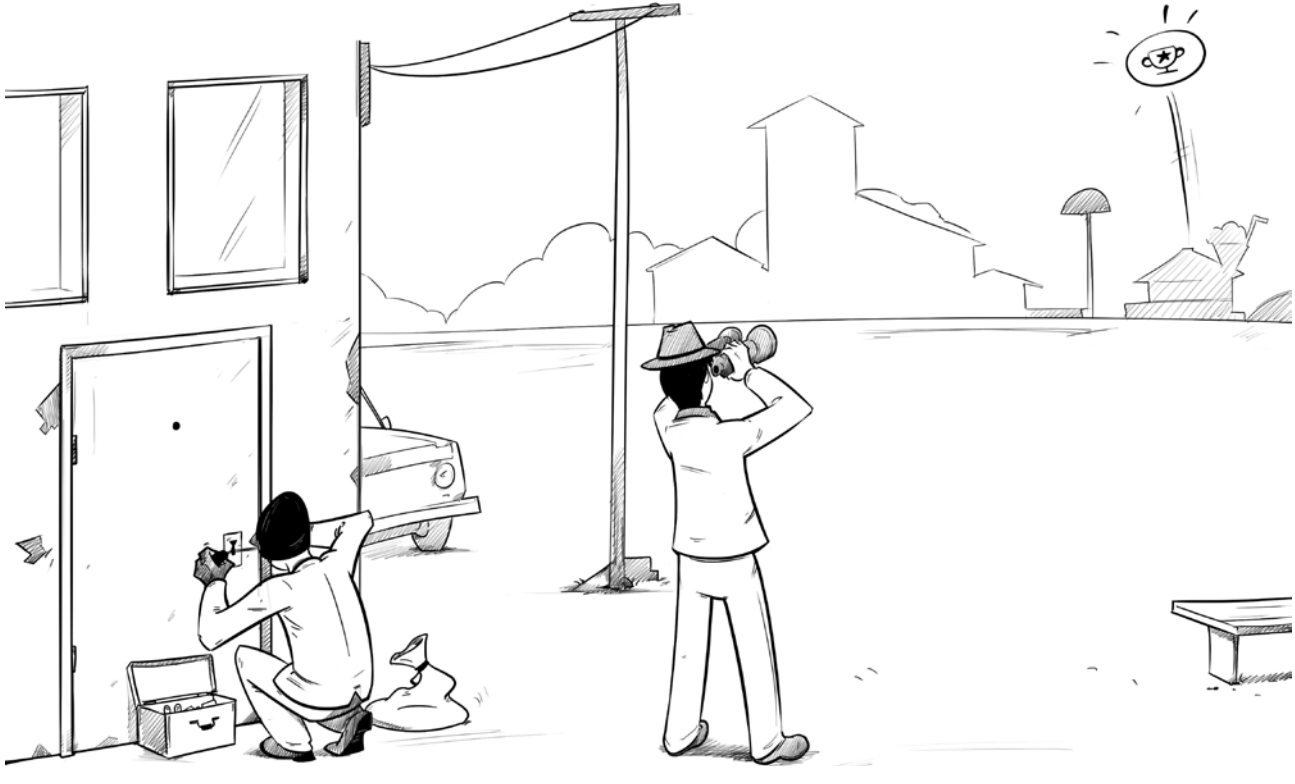
На сознательный обман могут пойти представители обоих полов, но бóльшая часть ограничится сравнительно безобидным ретушированием фотографии или изменением даты рождения. Гораздо хуже, если потенциальная вторая половинка окажется мошенником — в этом случае помимо времени вы рискуете потерять деньги, здоровье или даже жизнь. Впрочем, хороших людей в интернете также немало, и их можно найти, нужно лишь более внимательно подходить к выбору собеседника и не торопиться с личной встречей.

РОДИТЕЛЬСКИЙ КОНТРОЛЬ ЗАЩИЩАЕТ ОТ НЕЖЕЛАТЕЛЬНОГО ОБЩЕНИЯ

# СОВЕТ 21: **ОПАСНЫЕ ДРУЗЬЯ**

Если взрослый способен сам оградить себя от не очень умных людей из интернета, то ребенок, увы, может быть не очень разборчивым. Общение с неизвестными пользователями может быть не просто неприятным, а очень опасным, ведь ребенку неоткуда знать, что какой-нибудь общительный VinnieThePooh1967 на самом деле является закоренелым преступником-педофилом, ищущим повод для встречи с ребенком в уединенном месте. Если вы — родитель, не забудьте настроить родительский контроль на фильтрацию контактов в программах для обмена сообщениями и социальных сетях.

ЧЕКИН В КАФЕ СООБЩИТ ВАШЕ МЕСТОПОЛОЖЕНИЕ НЕ ТОЛЬКО ДРУЗЬЯМ



# СОВЕТ 22: **ВИРТУАЛЬНАЯ СЛЕЖКА**

Если вас планируют ограбить предусмотрительные преступники, то за вами, за вашей квартирой, дачей или машиной сначала установят наблюдение. Впрочем, это муторное и небезопасное дело уже выходит из моды: подросло поколение высокотехнологичных воров, которым достаточно подписаться на ваши обновления в социальных сетях. Распространенная привычка чекиниться везде, куда бы ни занесло человека, этим темным личностям очень на руку. Перед очередным чекином задумайтесь, сколько из ваших «друзей» в Swarm, Altergeo или Facebook действительно ваши друзья и хорошо ли вы их знаете.


НЕ СТОИТ ВЫКЛАДЫВАТЬ В СЕТЬ ФОТОГРАФИИ ЛИЧНЫХ ДОКУМЕНТОВ...

# СОВЕТ 23: **БЕРЕГИТЕ ДОКУМЕНТЫ**

В наш информационный век многие живут нараспашку, развлекая как близких друзей, так и неведомых «фолловеров» и «френдов» регулярно публикуемыми фотографиями, видеороликами и подробными рассказами про свой распорядок дня. Забавно, но как раз друзья, скорее всего, приравняют ваши откровения к информационному шуму, а вот недруги всерьез заинтересуются этими данными. Порывшись в Сети, преступник может выудить ценнейшую информацию об объекте своей «охоты», иногда даже достаточную для изготовления поддельных документов. В суде жертва наверняка сможет доказать, что не она брала те четыре кредита, но неприятный осадок останется надолго.


...И ЦЕННОГО ИМУЩЕСТВА
1200 $
340 $
2700 $

# СОВЕТ 24: **КРАСИВАЯ ЖИЗНЬ**

Благодаря развитию интернета криминальная профессия наводчика стремительно теряет свою востребованность: в наше время жертва сама выкладывает в интернет фотографии роскошного интерьера своей квартиры, новой машины или дорогого ноутбука. А потом еще и сообщит, что на следующей неделе улетает со второй половинкой в теплые края, то есть оставит ценности без присмотра. Представители преступного мира не хуже нас, честных людей, умеют пользоваться социальными сетями, тем более, что им они могут принести весомую материальную выгоду. В интернете безопаснее быть скромнее, да и вне его такое качество никому не вредит.


ЗЛОУМЫШЛЕННИКИ ГОТОВЫ КРАСТЬ ДАЖЕ ВНУТРИИГРОВОЕ ИМУЩЕСТВО

# СОВЕТ 25: **КРАЖА ИГРОВЫХ ДАННЫХ**

Некто взломал ваши учетные записи в онлайн-играх, украл навороченный меч, угнал любимый танк и увел со двора свинью девятого уровня? Удивляться нечему, закон рынка гласит: всякая вещь стоит столько, сколько за нее готовы заплатить. Поэтому игровые аккаунты и даже предметы из популярных игр, добыть которые можно лишь с большим трудом или по большому везению, могут иметь очень и очень большую ценность. Крадут у вас не пиксели, крадут у вас ваше время и труд, и если вы цените их, озаботьтесь адекватной защитой вашего цифрового имущества. Начните с усложнения паролей, и то же самое проделайте с электронной почтой, привязанной к игровым учетным записям.


ВНИМАТЕЛЬНО ФОРМИРУЙТЕ ПОИСКОВЫЕ ЗАПРОСЫ

# СОВЕТ 26: **ПРАВИЛЬНЫЙ ПОДХОД К ПОИСКУ**

Человеку свойственно ошибаться, в том числе и в наборе поисковых запросов. Поисковые системы уже научились подсказывать пользователю правильный вариант, но следует учесть, что против них работают лучшие умы киберпреступной отрасли, тщательно продумывающие, на какие запросы сделать свою ставку. В лучшем случае, опечатавшись в наборе запроса, вы найдете не то, что искали, и гораздо хуже, если предложенная вам страница будет выглядеть в точности так, как вы ожидаете, но по сути своей будет мошеннической или вредоносной. Ведь это означает заражение компьютера, потерю личных данных, а зачастую и денег.


ОБРАЩАЙТЕ ВНИМАНИЕ НА АДРЕС САЙТА

# СОВЕТ 27: **САЙТЫ-ФАЛЬШИВКИ**

Фишинг — заманивание жертвы на поддельный сайт — это излюбленная тактика киберпреступников. Совсем несложно сделать сайт, который внешним видом будет точно копировать популярный ресурс, например «Одноклассников» или Facebook, а затем разместить его по адресу, отличающемуся от настоящего всего парой букв. Далее дело за малым — разослать максимальному количеству пользователей письма от имени сайта, например с просьбой срочно сменить пароль от «Одноклассников» и ссылкой на сайт-обманку. Поверите мошенникам — и ваша страница в социальной сети перестанет быть вашей. Антивирусные компании постоянно ищут и блокируют фишинговые страницы, но глаза в интернете лучше держать открытыми.


НЕ ДОВЕРЯЙТЕ СООБЩЕНИЯМ САЙТОВ О ЗАРАЖЕНИИ КОМПЬЮТЕРА

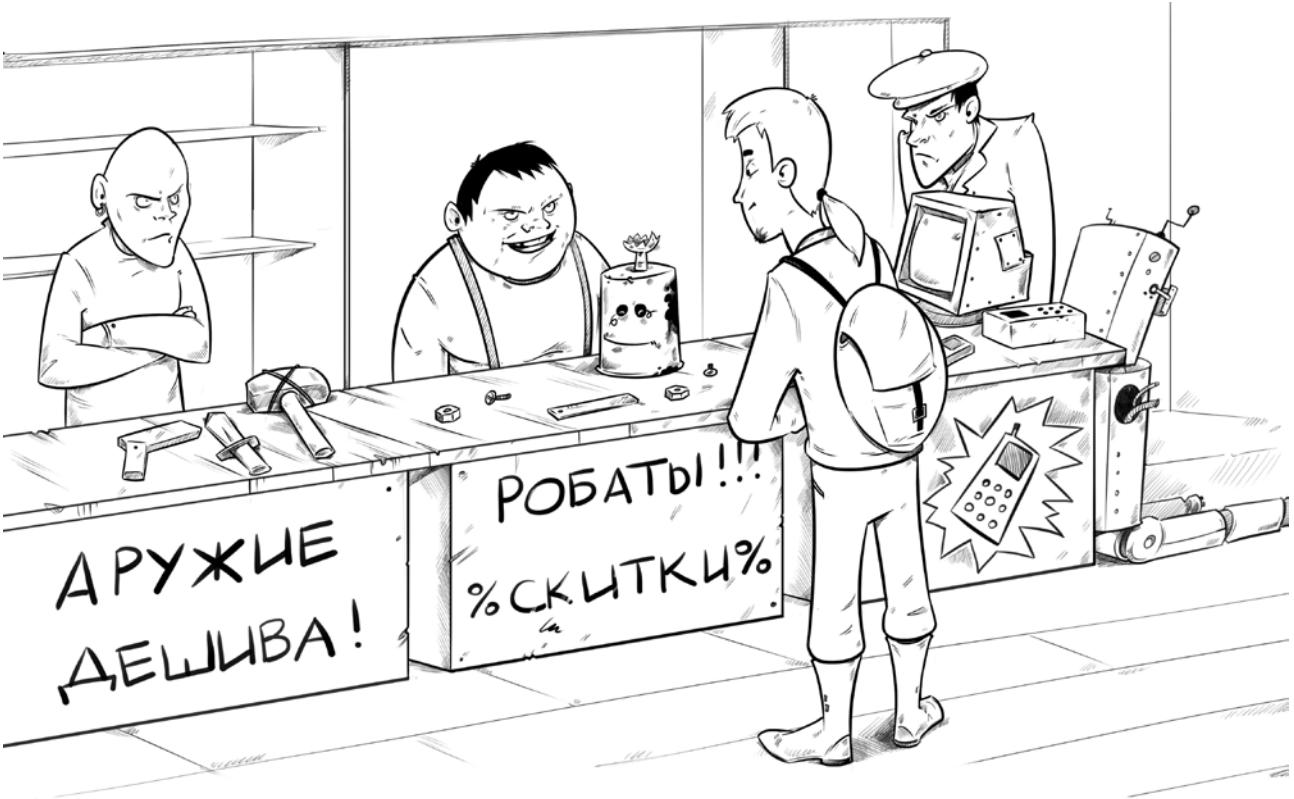
# СОВЕТ 28: **МОШЕННИЧЕСКИЕ ОПОВЕЩЕНИЯ**

Загрузив новый сайт и увидев на нем пестрый баннер с предупреждением о вирусах на вашем компьютере, не спешите пугаться и соглашаться на все, что хитрый баннер вам предложит. Ну посудите сами, откуда баннеру знать такие вещи? Все это он выдумывает, чтобы вынудить вас согласиться на загрузку некоего чудо-антивируса. Вот как раз после этого вирусы у вас и появятся, поскольку с помощью таких баннеров и распространяется вредоносное программное обеспечение. Лучшим вариантом будет просто закрыть как надоедливый баннер, так и показавший его сайт — все равно ничего хорошего вы там не найдете.

# БАННЕРОРЕЗКА ИЗБАВИТ ОТ ОПАСНЫХ СОБЛАЗНОВ

# СОВЕТ 29: **ИНТЕРНЕТ БЕЗ БАННЕРОВ**

Ученые (возможно, британские) уже доказали, что реклама действует даже на тех, кто на нее не обращает никакого внимания. А это значит, что в ваших же интересах поскорее избавиться от многочисленных рекламных баннеров, украшающих веб-сайты и порой занимающих бóльшую часть окна браузера. Самые наглые, называемые поп-апами, так вообще полностью закрывают нужное окно, и выглядит это так же уместно, как раздатчик рекламы у метро, внезапно наклеивающий свою листовку прохожему на лицо. Чтобы не стать жертвой рекламы, стоит установить себе специальную программу, скрывающую баннеры. Они бывают как в виде отдельных приложений, так и в виде дополнений к браузерам. Следите только за тем, чтобы под видом баннерорезки не установить себе особенно лютое рекламное приложение. Также стоит помнить, что реклама помогает сайтам оставаться бесплатными, поэтому наиболее продуманные «баннерорезки» позволяют вам согласиться на просмотр неагрессивной рекламы.




ПОСЕЩАЙТЕ ТОЛЬКО ПОПУЛЯРНЫЕ, ПРОВЕРЕННЫЕ ИНТЕРНЕТ-МАГАЗИНЫ...

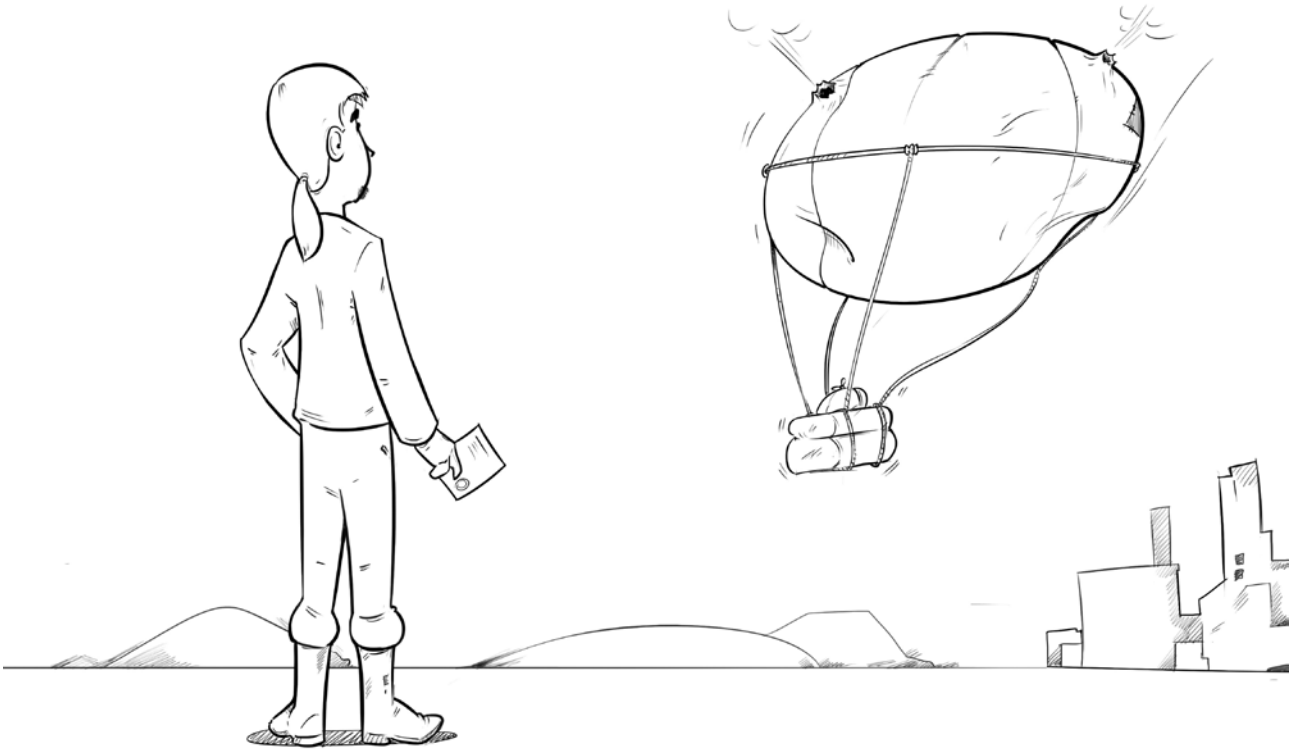
# СОВЕТ 30: **ПОДДЕЛЬНЫЕ МАГАЗИНЫ**

Труд злоумышленника несложен: скопировать содержимое интернет-магазина, слегка изменить, разместить на своем домене, чуток «раскрутить» — и собирай с посетителей их имена, адреса, контактную информацию, а то и данные банковских карт. А если на странице оплаты товара будут варианты перевода денег на электронный кошелек, то и деньги начнут сыпаться. Все это делается так просто и легко, что становится страшновато приобретать что-либо через интернет.
На самом деле есть несколько правил, как не попасть впросак в таких случаях, и одно из них состоит в том, что не стоит идти за покупками в такое глухое место, где еще никому ничего не удалось приобрести. Пользуйтесь проверенными, известными магазинами.


...ИМЕЮЩИЕ СЕРТИФИКАТЫ БЕЗОПАСНОСТИ

# СОВЕТ 31: **БЕЗОПАСНЫЙ ШОПИНГ**

Правильный интернет-магазин непременно использует защищенный протокол HTTPS с сертификатом, подписанным легальным удостоверяющим центром. Убедиться в наличии такового совсем несложно — достаточно посмотреть на адресную строку. Если там значится «https://...» и светится иконка шифрования (обычно это зеленый замочек), вы пришли куда надо. HTTPS защищает от множества угроз: подмены всего сайта, перехвата передаваемой информации, подмены отправляемых и получаемых данных.



И НЕ ЗАБУДЬТЕ УТОЧНИТЬ ВОЗМОЖНОСТЬ ДОСТАВКИ И ЕЕ СТОИМОСТЬ

# СОВЕТ 32: **МОШЕННИКИ НА ДОСТАВКЕ**

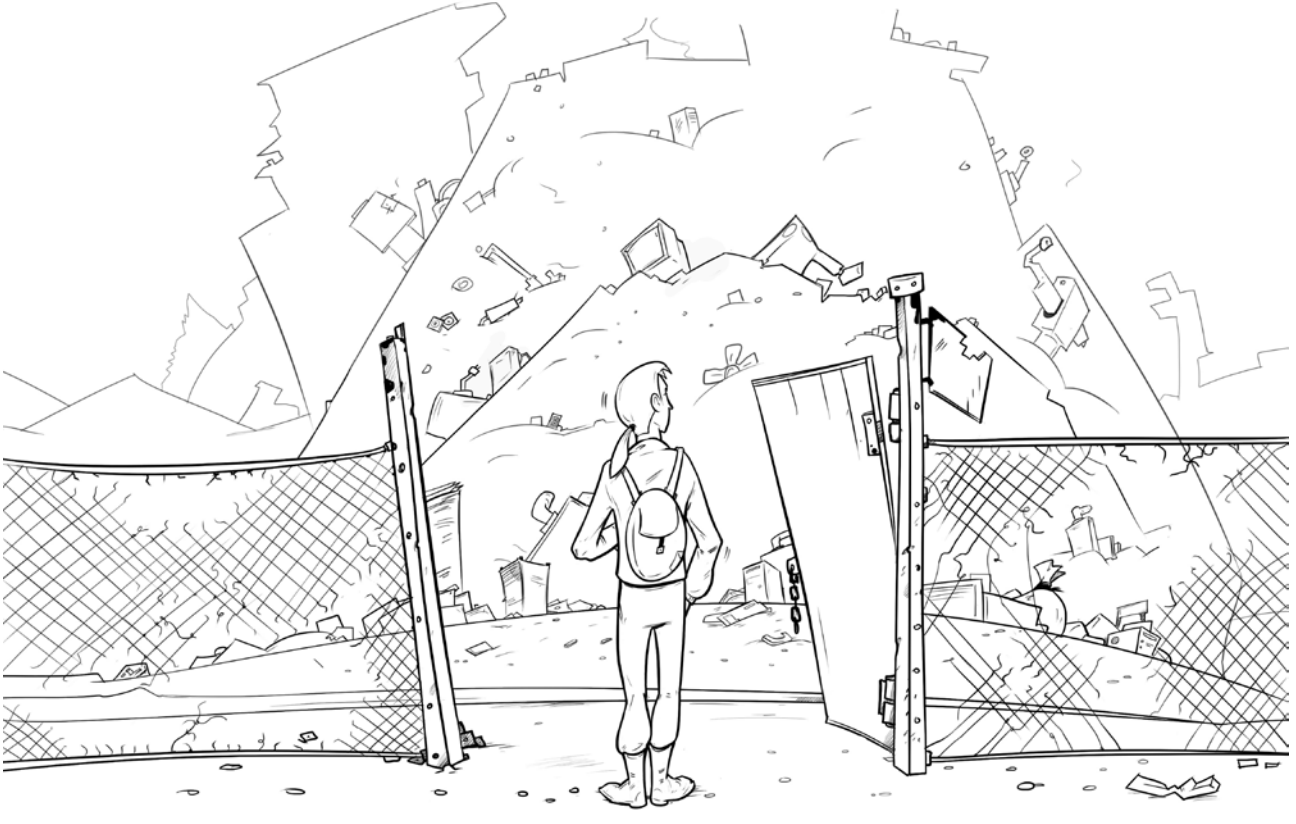
Многие не раз попадали в ситуацию, когда после заказа товара в интернет-магазине товар то отгружался, то передавался курьеру, то внезапно оказывался отсутствующим на складе. Это может быть как сбоем в торговой системе магазина, так и уловками злоумышленников, которые не собираются что-то кому-то продавать, а лишь собирают данные потенциальных жертв. Так или иначе, если товар уже оплачен посредством банковской карты или электронного кошелька, такие фортеля службы доставки могут заставить клиента изрядно понервничать. Стоит ли удивляться, что самым популярным методом оплаты в России по-прежнему остается оплата наличными курьеру после вручения и проверки товара?

ДОСТУП К ВАШЕЙ БАНКОВСКОЙ КАРТЕ ОБЕСПЕЧИТ РЕБЕНКУ
ВЕСЕЛЫЙ ШОПИНГ

# СОВЕТ 33: **БАНКОВСКИЕ КАРТЫ И ДЕТИ**

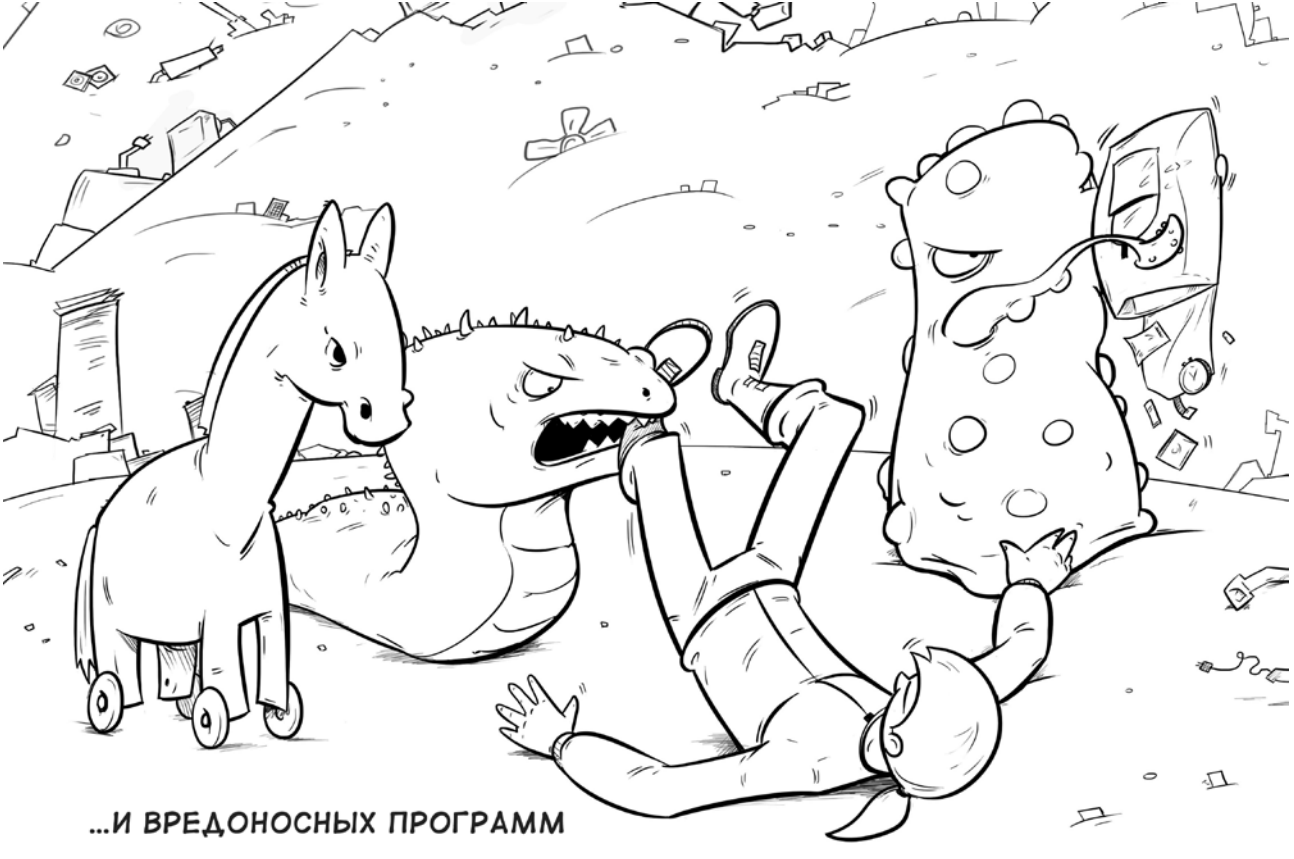
Оплачивать покупки в интернете с помощью банковской карты весьма удобно, особенно когда магазин позволяет привязать карту к аккаунту и не вводить каждый раз все данные заново. Но тогда не удивляйтесь, если вдруг обнаружите счета за незнакомые покупки, например полную дискографию Димы Билана. Это лишь означает, что ваши дети научились пользоваться вашей банковской картой и освоили мир интернет-шопинга. Даже в обычных магазинах продавцы не склонны спрашивать документы при оплате по карте, а уж в интернете можно найти множество сервисов, принимающих карты безо всяких дополнительных паролей и кодов подтверждения. Принимайте меры — деньги и детей до определенного возраста лучше держать раздельно.

ТОРРЕНТ-ТРЕКЕР — КЛАДЕЗЬ ПОЛЕЗНОЙ ИНФОРМАЦИИ...



# СОВЕТ 34: **СКЛАД ФАЙЛОВ**

Торрент-трекер — это каталог ссылок или форум, на котором любители бесплатного обмена файлами выкладывают ссылки на скачивание полезных программ, фильмов, игр, книг и многого другого. Загрузка нужного файла производится с помощью специальной программы (торрент-клиента), причем файл скачивается с компьютеров сразу нескольких пользователей торрент-трекера, уже загрузивших этот файл ранее. На трекере можно найти контрафактную копию коммерческой программы, экранную копию свежайшего голливудского фильма, контент для взрослых и даже что-нибудь совсем незаконное. В некоторых странах Европы активными пользователями торрент-трекеров уже начали интересоваться правоохранительные органы, а в России такие ресурсы регулярно блокируются Роскомнадзором. В общем, все достоинства и недостатки бесплатного сыра налицо.


...И ВРЕДОНОСНЫХ ПРОГРАММ

# СОВЕТ 35: **ОПАСНОСТИ ТОРРЕНТОВ**

Есть у торрент-трекера и темная сторона. Каждый такой сайт содержит ссылки на многие терабайты всяких разных файлов, причем выложить что-то новое может кто угодно. Потому перед тем, как скачивать что-либо оттуда, спросите себя, готовы ли вы доверять этому «кому угодно»: в красиво оформленной раздаче может таиться троянская программа, которая моментально выпотрошит ваш банковский счет или заблокирует компьютер, а затем потребует выкуп за разблокировку. Для киберпреступников любой торрент-трекер представляет собой удобный, быстрый и анонимный способ распространения вредоносных программ. Правда, многих пользователей торрент-трекеров это не останавливает.

СДЕЛАЛИ ДЕЛО — ОЧИСТИТЕ КУКИ!

# СОВЕТ 36: **ЧИСТЫЙ БРАУЗЕР**

Стоило зайти на сайт банка, как баннеры на всех сайтах запестрели предложениями выгодных вкладов и доступных кредитов? Никакой магии, причина в cookie — небольших текстовых файлах, необходимых сайтам, чтобы запоминать пользователей и их предпочтения. Но кроме того, они могут использоваться третьей стороной для отслеживания действий пользователя в интернете, что очень любят проделывать рекламные баннерные сети. И, что самое неприятное, укравшие их злоумышленники смогут притвориться вами, даже не зная логина и пароля от вашей учетной записи на сайте. Добавьте к этому тот факт, что cookie могут «жить» в вашем браузере годами, и станет понятно — от них следует своевременно избавляться, благо все современные браузеры обладают функцией удаления cookie.


ПРИВАТНЫЙ РЕЖИМ БРАУЗЕРА СКРОЕТ ЗАПРОСЫ
И ИСТОРИЮ ПОСЕЩЕНИЯ

# СОВЕТ 37: **ПРИВАТНЫЙ ИНТЕРНЕТ**

Мы не спрашиваем, чем вы занимаетесь в интернете, и другим интересоваться не советуем, ведь каждому нужно немного личного пространства, даже виртуального. Однако ваши cookie и история сайтов, которые вы посещаете, могут служить не только для вашего удобства, но и для отслеживания вашей деятельности в интернете. Замести следы можно, тщательно «подчищая» за собой, но иногда удобнее совсем не оставлять следов — для этого нужен приватный режим браузера. Это особенно полезно, если за вашим компьютером иногда работают и другие пользователи.


ПРИ РАБОТЕ С ЧУЖИМ КОМПЬЮТЕРОМ
ИСПОЛЬЗУЙТЕ МИНИМУМ ЛИЧНОЙ ИНФОРМАЦИИ...

# СОВЕТ 38: **НЕ ОСТАВЛЯЯ СЛЕДОВ**

Любой компьютер впитывает в себя информацию, как губка воду, так уж он устроен. И если вы оказались за чужим компьютером, не стоит забывать, что может найтись умелец, который выжмет эту губку и завладеет ценными данными, в том числе и вашими. И неизвестно, в чьи руки в конечном итоге попадет список посещенных вами страниц, ваши логины и пароли, написанные вами письма и сообщения. Это не значит, что общедоступным компьютером пользоваться нельзя, следует лишь помнить, что это не просто недоверенная, а потенциально враждебная среда. Немного здоровой паранойи определенно не повредит.


...И ПОМНИТЕ, ЧТО ОБЩЕДОСТУПНЫЕ КОМПЬЮТЕРЫ МОГУТ БЫТЬ ЗАРАЖЕНЫ

# СОВЕТ 39: **ОБЩЕДОСТУПНЫЙ ВИРУС**

Работая за чужим компьютером, можно не только оставить там что-то ценное, но и заполучить оттуда что-то неприятное. Речь, конечно, о вредоносных программах, которыми может быть заражена общедоступная система. Распространяться зловреды умеют по-всякому, и вставленная в USB-порт личная флешка может за доли секунды превратиться в переносчика опасной заразы. Ведь неизвестно, что было на тех флешках, что вставляли в этот компьютер до вас другие пользователи, и какие сайты в интернете они посещали.

ОБЩЕСТВЕННЫЙ WI-FI — ВСЕ РАВНО ЧТО ОБЩЕСТВЕННЫЙ БАССЕЙН

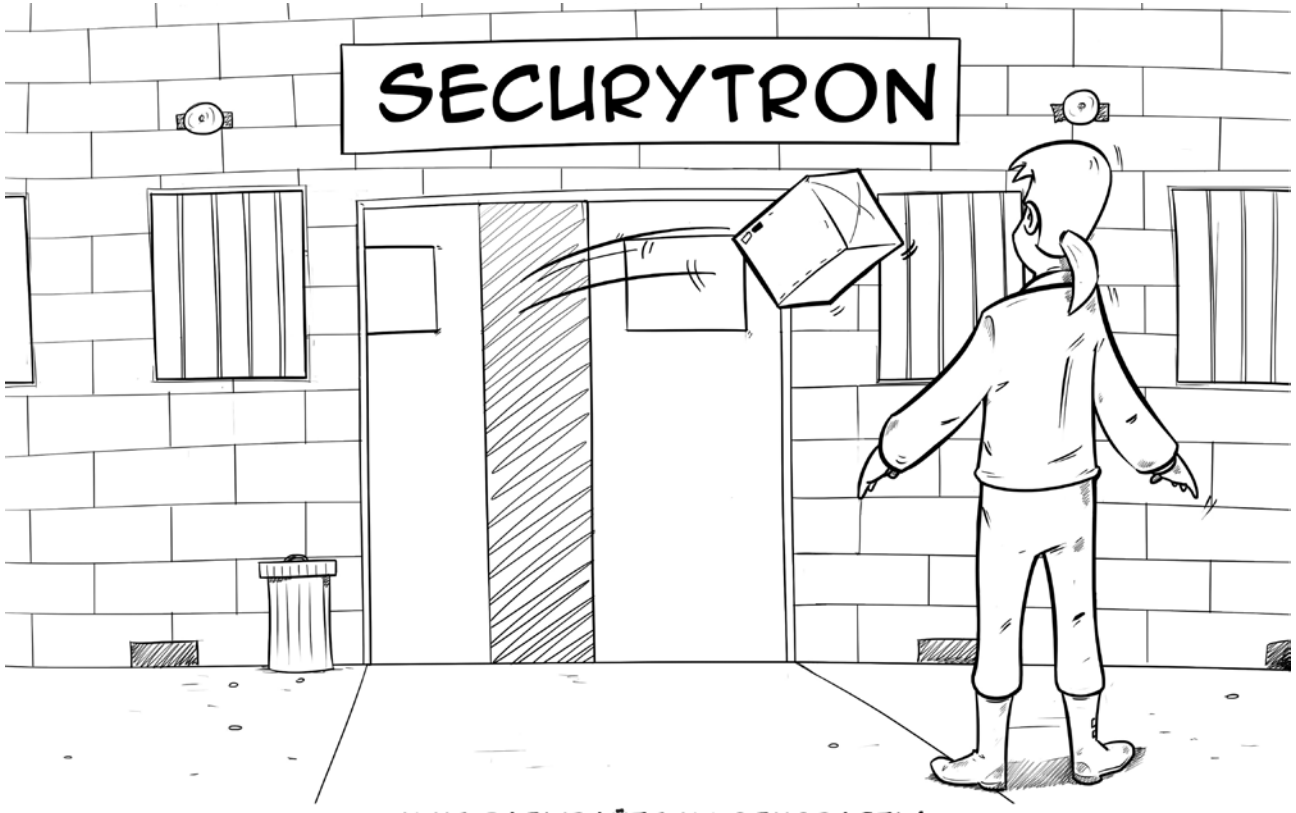
# СОВЕТ 40: **В ОБЩЕСТВЕ ХАКЕРА**

Общественный Wi-Fi зачастую лучше мобильного интернета, поскольку обеспечивает более быстрый доступ в Сеть и, главное, бесплатен. Вот только этот канал связи, как правило, плохо защищен и не принадлежит вам лично, то есть его настройки неизвестны и его приходится делить со множеством людей вокруг. Увы, среди них могут быть и злоумышленники, охочие до чужой личной информации и знающие, как устроить перехват данных в незащищенных беспроводных сетях. И самое неприятное, что об их существовании вы узнаете только в тот момент, когда преступники решат воспользоваться украденным паролями и устроить спам-рассылку с вашего почтового ящика или отредактировать ваш профиль в социальной сети.


СКАЧИВАЙТЕ ПРОГРАММЫ ТОЛЬКО С САЙТА ПРОИЗВОДИТЕЛЯ...

# СОВЕТ 41: **БЕЗОПАСНОЕ СКАЧИВАНИЕ**

Если вам приглянулась полезная программка, не стоит скачивать ее по первой ссылке, выданной поисковиком, — программа, возможно, будет работать, вот только вместе с ней вам завернут неприятный сюрприз. Ведь один из способов распространения вредоносных и надоедливых рекламных программ заключается в их внедрении в популярные приложения. Злоумышленники активно «раскручивают» веб-сайты с зараженными приложениями, в результате чего поисковые системы могут показывать их выше, чем официальные веб-страницы производителей этих программ. Так что если вам лень тратить время на поиск официального сайта, задумайтесь, стоит ли потакать лени, если на кону ваш компьютер и личные данные.




...И НЕ ЗАБЫВАЙТЕ ИХ ОБНОВЛЯТЬ!

# СОВЕТ 42: **ЗАГРУЗКА ОБНОВЛЕНИЙ**

Единожды скачав программу, можно пользоваться ею многие годы — она не механизм, износу не подвержена. Но все-таки совсем расслабляться не стоит: любая программа содержит ошибки — уязвимости, которые могут быть использованы злоумышленниками для заражения компьютера. И чем популярнее программа, тем больше злоумышленников пытается найти в ней уязвимые места. В то же время и авторы, узнав, что в их приложении есть уязвимость, стремятся быстро выпустить новую версию без этой дыры. А это означает, что просто скачать программу мало, нужно своевременно устанавливать все доступные обновления.

ВО ВРЕМЯ УСТАНОВКИ ПРИЛОЖЕНИЯ
ВНИМАТЕЛЬНО ИЗУЧИТЕ ДОПОЛНИТЕЛЬНЫЕ ОПЦИИ ИНСТАЛЛЯТОРА...

# СОВЕТ 43: **ПРАВИЛЬНАЯ УСТАНОВКА ПРОГРАММ**

Бесплатные программы радуют кошелек, но жизнь такова, что их авторам тоже надо на чем-то зарабатывать. Потому многие разработчики разрешают дополнять установку своей программы различными посторонними приложениями, панелями инструментов и дополнениями к браузерам, которые в лучшем случае завалят вас ненужными инструментами, мешающими нормальной работе, а в худшем — замучают рекламными баннерами.

...УСТАНОВКУ ДОПОЛНИТЕЛЬНЫХ МОДУЛЕЙ ЛУЧШЕ СРАЗУ ОТМЕНИТЬ

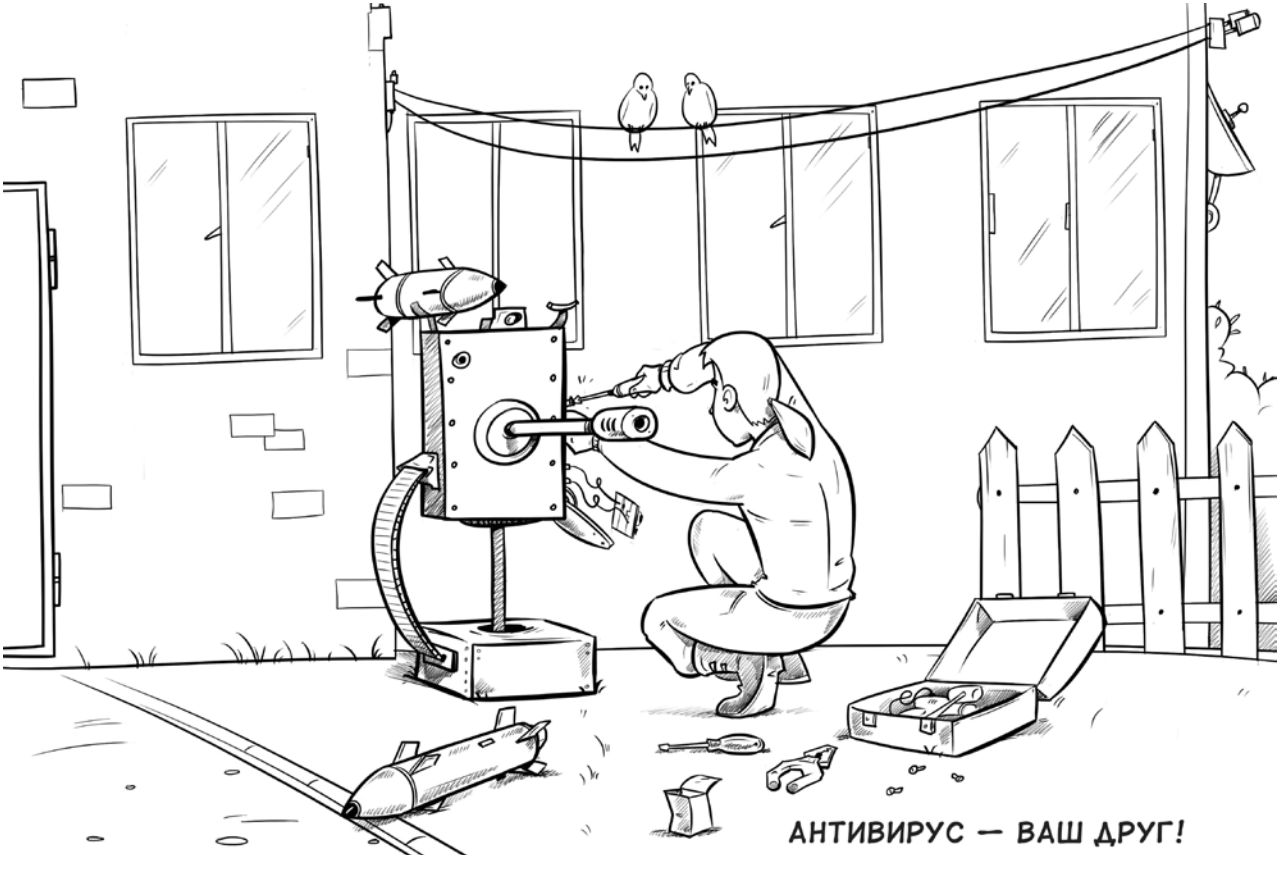
# СОВЕТ 44: **ПРОГРАММЫ БЕЗ МУСОРА**

А теперь хорошая новость: почти всегда установку сопутствующего барахла можно отменить в установщике исходной программы, нужно лишь изменить его настройки. Потому во время установки любого приложения стоит читать появляющиеся на экране сообщения и внимательно изучать окна инсталлятора, и тогда не придется потом вычищать систему от непосильного груза десятков бесполезных, а иногда и откровенно вредных дополнений.


ЧИТАЙТЕ ЛИЦЕНЗИОННЫЕ СОГЛАШЕНИЯ, ВКЛЮЧАЯ ПРИМЕЧАНИЯ

# СОВЕТ 45: **ПРОВЕРКА СОГЛАШЕНИЯ**

Полезная программа, за которую вы честно выложили солидную сумму, запросто может обладать скрытыми функциями, работающими отнюдь не в вашу пользу. Или другая ситуация: программа работает с вашими данными, но ее разработчики не хотят отвечать за их сохранность, зато очень хотят поставлять сведения о вас рекламодателям. В таких случаях разработчики тщательно продумывают текст лицензионного соглашения, чтобы он максимально освобождал их от возможной ответственности. Мы советуем внимательно читать эти запутанные документы, причем до установки самой программы — так вы можете изрядно облегчить себе жизнь.


АНТИВИРУС — ВАШ ДРУГ!

# СОВЕТ 46: **БАЗОВАЯ ЗАЩИТА**

Пожалуй, каждый обитатель собственного дома или владелец дачи хоть раз мечтал об автоматической оборонительной системе, способной удерживать на расстоянии выстрела воров и продавцов краденного садового инструмента, шумные компании малолетней шпаны и назойливых соседей. В реальности это запрещено законом, да и негуманно, а вот в кибермире без подобной системы не обойтись. Антивирусное ПО защитит компьютер от информационных угроз и нежелательного внимания спамеров, что позволит вам спокойно работать, учиться и развлекаться в информационном пространстве интернета.

НЕ ДОВЕРЯЙТЕ ЗАБОТУ О ДРУГЕ НЕЗНАКОМЫМ «КОМПЬЮТЕРЩИКАМ»

# СОВЕТ 47: **НАСТРОЙКА АНТИВИРУСА**

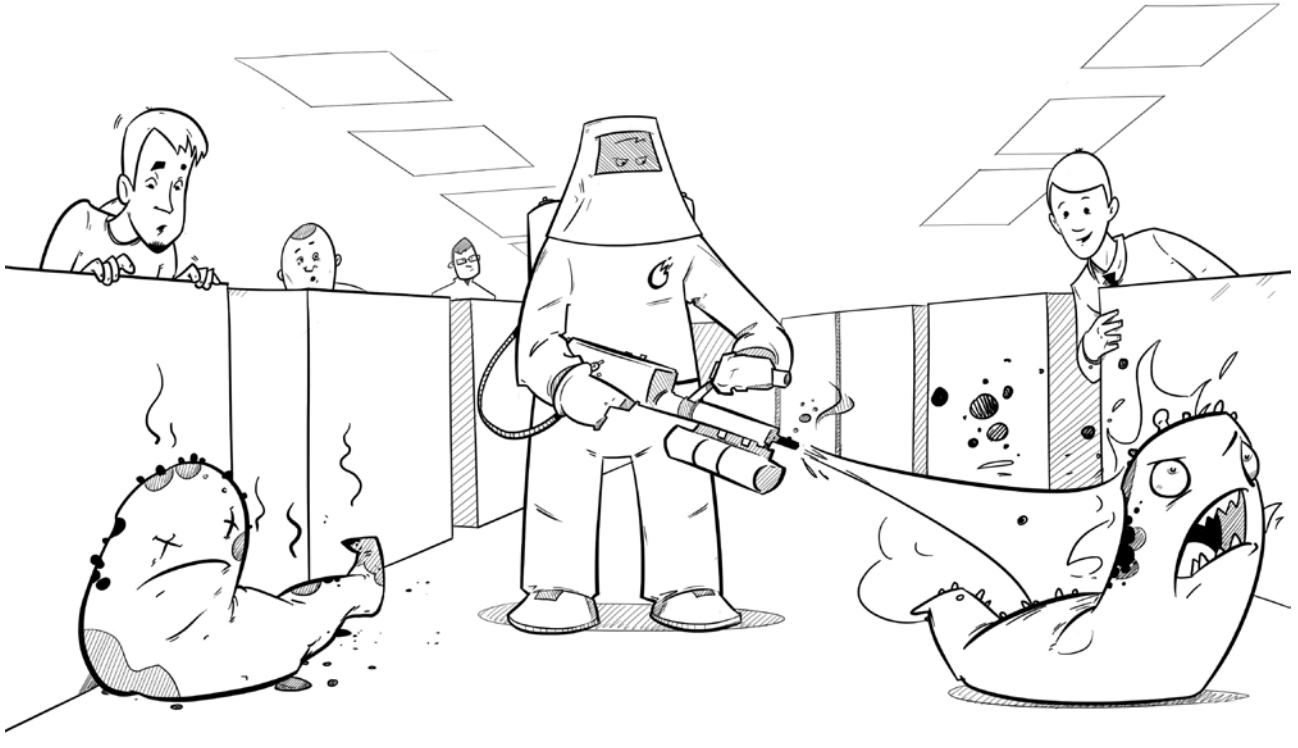
Кто готов доверить свои деньги, документы и личные тайны первому встречному незнакомцу? В здравом уме и твердой памяти, наверное, никто. Сегодня в список ценностей можно смело включить и персональный компьютер, который для многих стал и электронным кошельком, и личным дневником. Поэтому к настройкам компьютера, и особенно установленных на нем защитных инструментов, не стоит подпускать кого попало. И проблема даже не столько в возможном злом умысле, сколько в ответственном подходе к делу: безалаберная настройка параметров может лишить вас защиты от информационных угроз.

КОМПЛЕКСНОЕ ЗАЩИТНОЕ РЕШЕНИЕ
ИЗБАВИТ ВАС ОТ ЛЮБЫХ НЕЖЕЛАТЕЛЬНЫХ ГОСТЕЙ

# СОВЕТ 48: **НАДЕЖНАЯ ЗАЩИТА**

Интернет — очень опасное место. Откроешь дверь хорошенькой программке, а за ней обязательно увяжется какой-нибудь подозрительный гость, который тут же заявит права на реестр вашей операционной системы, перетряхнет жесткий диск, забьет браузер рекламой и затребует с вас же денег за возможность беспрепятственно работать с компьютером. Таких гостей мы советуем отстреливать еще до того, как они шагнут за порог, только старайтесь, чтобы при этом не пострадали полезные приложения. Обеспечить надежную автоматическую охрану поможет антивирусный продукт, специально обученный отличать плохих от хороших и способный воздать каждой программе по заслугам.

ЗАЩИТУ РАБОЧЕГО МЕСТА ОБЕСПЕЧИТ СИСТЕМНЫЙ АДМИНИСТРАТОР



# СОВЕТ 49: **РАБОТА ПРОФЕССИОНАЛА**

Беспечные сотрудники — извечная головная боль системных администраторов. Они же как дети! То шнур выдернут, то кофе на клавиатуру прольют, то какой-нибудь вредоносный файл на компьютер загрузят. В последнем случае системный администратор всегда придет на помощь, главное, ему не мешать: предоставить доступ к рабочему месту и сообщить симптомы заболевания. Учтите, что фразы «я сейчас занят, давай позже», «только ни в коем случае не перезагружай!», «нет, эти 19 документов Excel закрывать нельзя» очень нравятся злоумышленникам, ведь они мешают сисадмину делать его работу по избавлению компании от информационных угроз.

ПОКИДАЯ РАБОЧЕЕ МЕСТО, БЛОКИРУЙТЕ КОМПЬЮТЕР

# СОВЕТ 50: **БЕЗОПАСНОСТЬ НА РАБОТЕ**

Любой человек, севший на ваше рабочее место в ваше отсутствие, будет воспринят компьютерами компании как вы. Чтобы эта неприятность произошла, достаточно оставить систему незаблокированной на время обеденного перерыва! По возвращении вас могут ожидать неприятные сюрпризы: коллеги-шутники наверняка написали от вашего имени гадостей боссу или отправили на принтер с вашего компьютера «Властелина колец» с цветными иллюстрациями. Причем это еще позитивный сценарий, будет гораздо хуже, если до компьютера доберется некто с недобрыми намерениями. А ведь всего-то нужно было нажать две клавиши перед уходом с рабочего места!


НЕНУЖНЫЕ ДОКУМЕНТЫ СКАРМЛИВАЙТЕ ШРЕДЕРУ

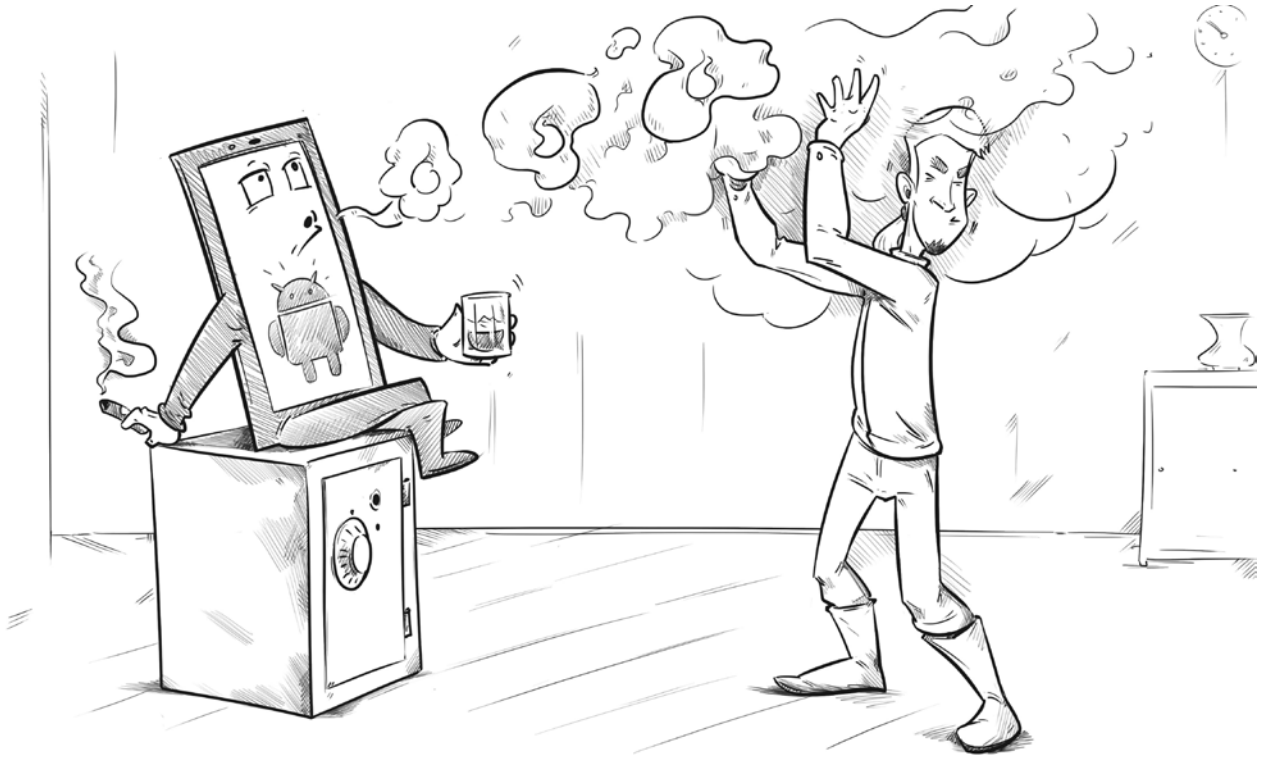
# СОВЕТ 51: **НЕЦИФРОВЫЕ ДОКУМЕНТЫ**

Что для вас мусор, для преступника может стать источником бесценной (точнее, очень дорогой) информации. Старые ненужные документы и распечатки рано или поздно оказываются на помойке, и если они не побывали перед этим в шредере, злоумышленники выудят из них множество сведений: оттиск печати организации, образцы подписей руководителей, адреса, имена и платежные реквизиты контрагентов, списки сотрудников и многое другое. Забыли покормить шредер? Не удивляйтесь потом, когда некто получит товар вместо вашего экспедитора или снимет деньги со счета организации.

«РУТОВАННЫЙ» СМАРТФОН УЯЗВИМ ДЛЯ ЗЛОВРЕДОВ

# СОВЕТ 52: **ВЗЛОМ СМАРТФОНА**

Современные мобильные ОС несколько ограничивают свободу владельца смартфона, например не дают ему возможность изменять системные файлы. Сбросить эти оковы помогает «взлом» смартфона и получение прав администратора — эта операция называется рутованием, или джейлбрейкингом. Однако преимущества расширенных прав ценят не только пользователи, но и многочисленные злоумышленники, специализирующиеся на угрозах для мобильных устройств. Атаковать взломанную ОС гораздо проще, а потому вероятность заражения для аппарата с получением root-доступа многократно возрастает. А теперь подумайте еще раз, действительно ли это вам так необходимо?



ПРЕЖДЕ ЧЕМ УСТАНОВИТЬ МОБИЛЬНОЕ ПРИЛОЖЕНИЕ,
ВНИМАТЕЛЬНО ИЗУЧИТЕ СПИСОК РАЗРЕШЕНИЙ

# СОВЕТ 53: **ВЫБОР ПРИЛОЖЕНИЯ**

Невинное приложение-калькулятор отправило в ваш банк SMS с командой на перевод ваших денег на незнакомый счет, а затем разослало по списку контактов телефона ссылки на свою копию? Неприятная ситуация. Но постарайтесь вспомнить, изучили ли вы список разрешений, запрашиваемых коварным приложением при установке? Наверняка нет, иначе вы бы задались вопросом, зачем какому-то калькулятору доступ к списку контактов и SMS. Увы, пользователи смартфонов часто игнорируют список запрашиваемых разрешений, добровольно разрешая приложению творить на устройстве все, что заблагорассудится его авторам. К счастью, одного дорогостоящего урока обычно хватает, чтобы начать относиться к этому чуть внимательнее.

БЕСПЛАТНЫЕ МОБИЛЬНЫЕ ПРИЛОЖЕНИЯ
МОГУТ СОВЕРШАТЬ ПОКУПКИ

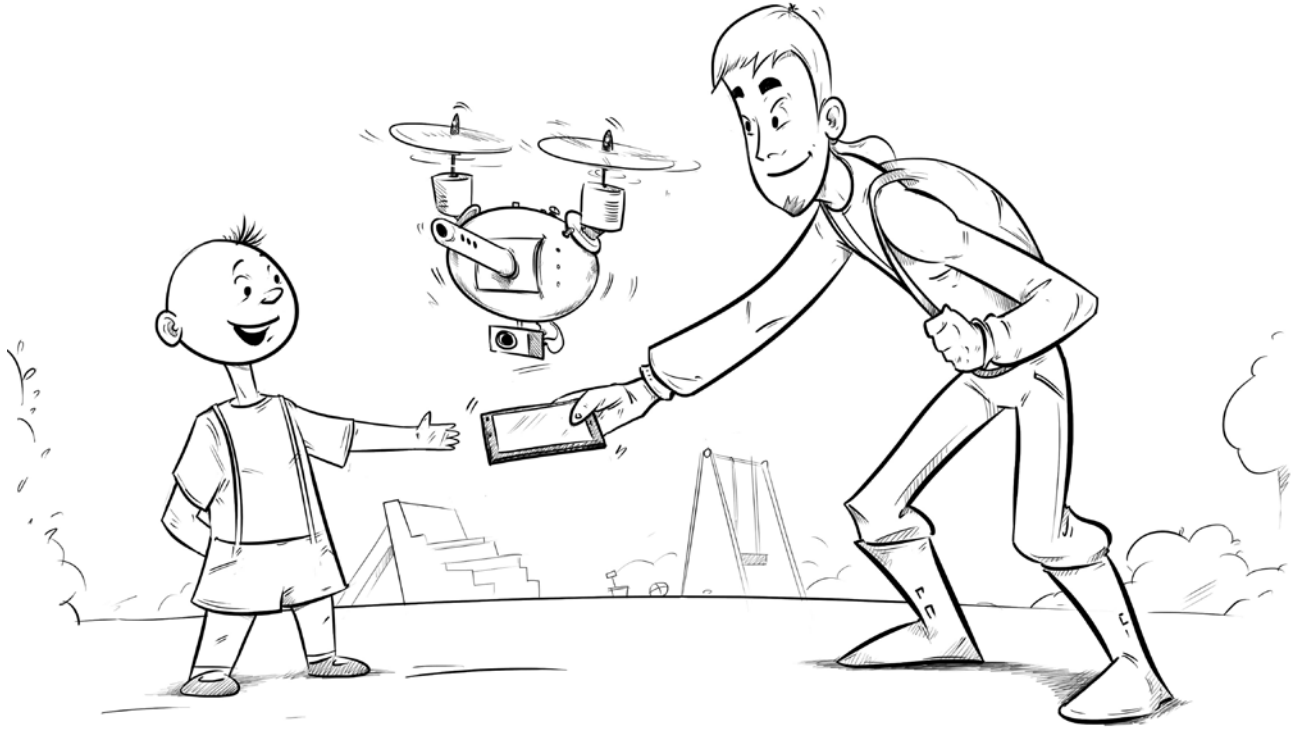
# СОВЕТ 54: **НЕЗАМЕТНЫЕ МОБИЛЬНЫЕ ПЛАТЕЖИ**

С ценой мобильных приложений не все так просто: если приложение можно скачать бесплатно, это еще не значит, что вы не потратите денег. Более того, вам оно может обойтись дороже любого платного. Если повезет, оно просто замучает вас показами рекламы, а если нет — «подоит» вашу банковскую карту покупками внутри приложения. Это вполне легально с точки зрения компаний — владельцев магазинов мобильных приложений, ведь многие пользователи действительно с легкостью готовы потратить доллар-другой на новый крутой меч в любимой игре. Нужно только сделать так, чтобы покупка происходила пусть и в явном виде, но быстро и безболезненно. А вот бесчестные разработчики предпочитают создавать приложения, способные совершать покупки и без вашего на то дозволения.

НЕ СТОИТ КЛИКАТЬ ПО НЕЗНАКОМЫМ ССЫЛКАМ В SMS

# СОВЕТ 55: **ОПАСНЫЕ SMS-СООБЩЕНИЯ**

Часто ли вы отправляете друзьям SMS со ссылкой на что-то интересное? Вряд ли. Зато злоумышленники просто обожают рассылать сообщения, содержащие вредоносную ссылку и текст, мотивирующий кликнуть по ней. Более того, они могут сделать так, что вредоносное сообщение придет с номера одного из ваших знакомых! Это, конечно, не значит, что злоумышленники склонили их к преступному заработку. Скорее всего, знакомому такая ссылка пришла чуть раньше, и он кликнул по ней. Теперь его смартфон заражен вредоносной программой, которая тут же принялась отправлять ссылки на себя по всему списку контактов.



НЕ ЗАБУДЬТЕ ПРО  ЗАЩИТУ ДЕТСКИХ МОБИЛЬНЫХ УСТРОЙСТВ

# СОВЕТ 56: **ЗАЩИТА ДЕТСКОГО СМАРТФОНА**

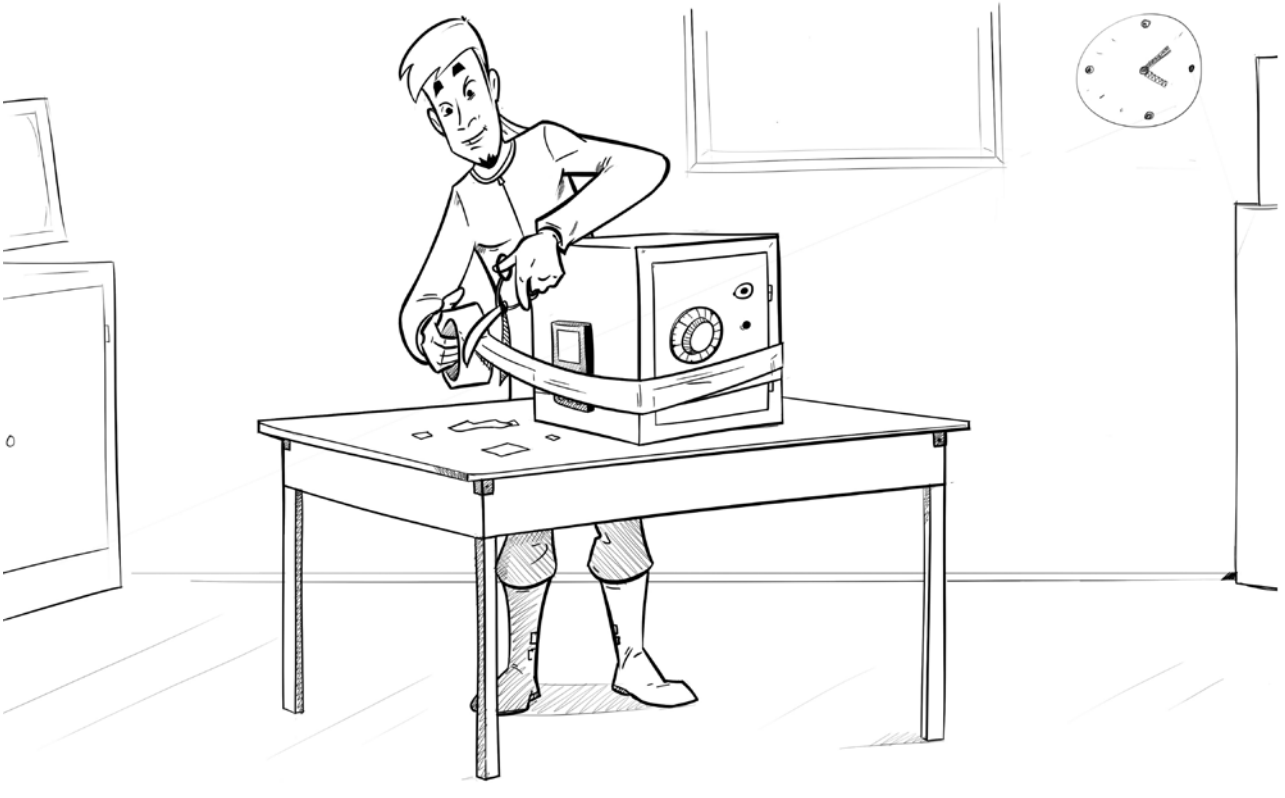
Ваш смартфон надежно защищен, а деньги с банковской карты все равно утекают из-за каких-то подозрительных покупок в Google Play... Нет, Google не пытается обворовывать вас по-тихому, это против принципов уважаемой компании. Самое время вспомнить, как вы ввели данные своей карты на телефоне ребенка для покупки пары детских игр. Теперь до детского телефона добралась мобильная зараза и потихоньку тянет деньги с карты, а возможно, и с мобильного счета. Самое время прекратить ее работу и установить на смартфон мобильный антивирус. Не оставляйте без защиты гаджеты ребенка!


ИСПОЛЬЗУЙТЕ АВТОРИЗАЦИЮ ПО ОТПЕЧАТКУ ПАЛЬЦА

# СОВЕТ 57: **НОВЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ**

По остросюжетным фильмам мы знаем, что обладатели замков с открытием по отпечатку пальца рано или поздно лишаются руки, а также «подзамочных» ценностей, но на практике ничего такого не случается. По сути, защита по отпечатку куда надежней четырехзначного цифрового кода или графического ключа, подсмотреть которые не составляет никакого труда. Особенно ненадежны простые защитные коды, если в роли «злоумышленника» выступает ваша вторая половина, которой очень захотелось прочитать SMS-сообщения на вашем смартфоне. Отпечаток удобен для владельца и неудобен для злоумышленников — двойной выигрыш.

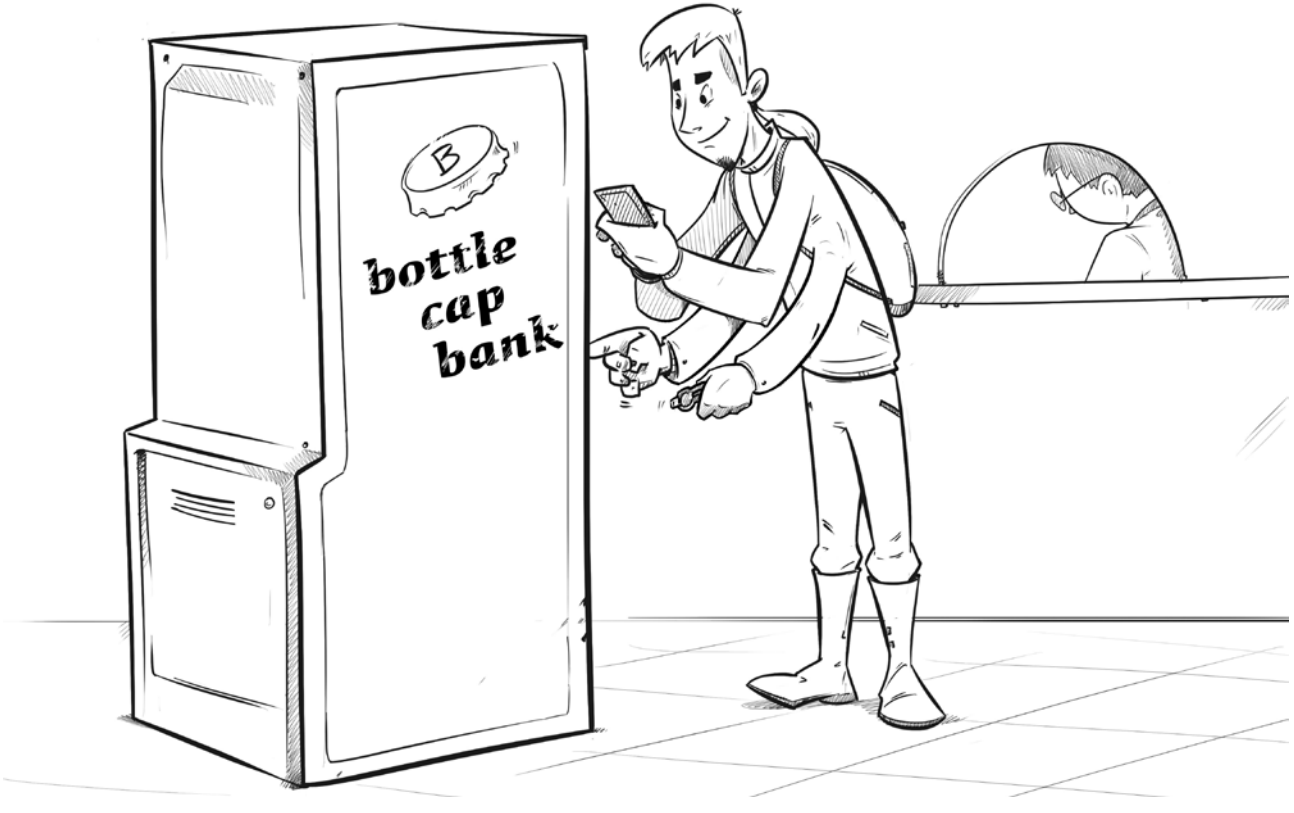
ПОДКЛЮЧИТЕ УСЛУГУ SMS-УВЕДОМЛЕНИЙ ОБ ОПЕРАЦИЯХ ПО КАРТЕ



# СОВЕТ 58: **КТО ПРЕДУПРЕЖДЕН, ТОТ ВООРУЖЕН**

Банкоматы, онлайн-покупки, интернет- и мобильный банкинг и прочие финансовые технологии — лучшие друзья вора. Ваши, конечно, тоже, но если для вас это лишь удобство, то для него — источник заработка. Плохие ребята очень любят грабить, не приближаясь к своей жертве, это и быстро, и легко, и безопасно. Зато защититься от подобного ограбления проще, но при одном условии: если вы знаете, что вас грабят. И если ежедневно смотреть выписку по банковской карте способен не каждый, то получение автоматических SMS-уведомлений об операциях никаких усилий не требует. Увидели SMS с незнакомой покупкой? Бегом в банк, блокировать карту! Кроме того, безналичные деньги хороши еще и тем, что их можно вернуть, не гоняясь за вором.

ИСПОЛЬЗУЙТЕ ДВУХФАКТОРНУЮ АУТЕНТИФИКАЦИЮ



# СОВЕТ 59: **ДВОЙНАЯ ЗАЩИТА ДЕНЕГ**

При неблагоприятном для вас стечении обстоятельств умелый хакер сможет украсть почти любой пароль. Так что если важный для вас сервис предлагает двухфакторную аутентификацию, лучше согласиться. Дополнительный уровень защиты в виде, например, присылаемого по SMS одноразового кода, обезопасит вашу учетную запись. Хорошим вариантом будет использование специального USB-токена (ключа в виде флешки), без установки которого в USB-порт компьютера войти в банк или на сайт иного защищаемого сервиса не получится.

НЕЗАЩИЩЕННЫЙ БАНКОМАТ МОЖЕТ СТАТЬ ОРУДИЕМ КИБЕРПРЕСТУПНИКОВ

# СОВЕТ 60: **ОПАСНЫЙ БАНКОМАТ**

Жаль, что банки не пишут на картах краткий, но емкий девиз «Смотри, куда суешь!» — это, без сомнения, помогло бы предотвратить немало случаев мошенничества. Банковские карты — удобнейший способ платежа и в то же время простой и безопасный метод ограбления вашего банковского счета. Например, обычный человек на глаз никак не сможет определить, чист ли банкомат или оснащен скиммером — устройством для кражи данных карты. Преступники (их называют кардерами) давно научились мастерски скрывать и маскировать свою аппаратуру, устанавливаемую на банкоматы. Инженерные бригады навещают банкомат раз в месяц или еще реже, и за это время ушлые кардеры могут украсть данные карт многих сотен и даже тысяч его пользователей.


САМЫЙ БЕЗОПАСНЫЙ БАНКОМАТ — В ОТДЕЛЕНИИ БАНКА

# СОВЕТ 61: **ВЫБОР БАНКОМАТА**

Но не все банкоматы одинаково опасны: преступники-кардеры любят оставаться с банкоматом наедине, чтобы установить или снять свое оборудование без лишних свидетелей. Причем уединенным местом может оказаться и оживленный торговый центр, постоянные толпы нагруженных покупками людей и сонные охранники обеспечивают преступнику возможность прийти, сделать свое черное дело и уйти с деньгами или данными карт, среди которых может оказаться и ваша. Лучший банкомат — тот, который установлен в хорошо просматриваемом, охраняемом и проглядываемом камерами помещении банка.


ПЕРЕДАЧА ДАННЫХ ПО NFC МОЖЕТ БЫТЬ ИСПОЛЬЗОВАНА
ДЛЯ ЗАГРУЗКИ ЗЛОВРЕДА

# СОВЕТ 62: **ВЫСОКОТЕХНОЛОГИЧНАЯ УГРОЗА**

Порой создается впечатление, что все виды связи придуманы людьми лишь для того, чтобы кому-либо вредить. Интернет полон киберугроз, почтовые голуби еще в старину норовили нагадить на голову получателя сообщения, телефон и поныне широко применяется для глупых розыгрышей, а Почта России сумела объединить в себе все самые лучшие практики. Казалось бы, технология NFC (Near Field Communication, связь ближнего действия) должна быть совершенно безобидной хотя бы в силу того, что действует на расстоянии в считанные сантиметры. Но нет, уже появились методики, позволяющие перехватить передаваемые посредством NFC данные или заразить мобильное устройство. В общем, стоит следить за тем, к чему и к кому вы прислоняете свой навороченный смартфон.

ИСПОЛЬЗУЙТЕ МОДУЛЬ КОНТРОЛЯ УЧЕТНЫХ ЗАПИСЕЙ

# СОВЕТ 63: **ПРОФИЛИ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ**

Модуль контроля учетных записей пользователей — это полезный инструмент, который отслеживает все действия, выполняемые запущенными приложениями, и при обнаружении потенциально опасной активности, для выполнения которой необходимы права администратора, останавливает программу и выводит на экран запрос разрешения. С помощью этого модуля можно создать пользовательские учетные записи для всех членов семьи, что существенно упростит им общение с компьютером, а различным вирусам, наоборот, усложнит. Ведь даже в случае успешного заражения пользовательской записи зловред не получит права администратора и не сможет серьезно навредить.

АНТИВИРУС СДЕЛАЕТ ЧИЩЕ ДОРОГУ К ЗНАНИЯМ

# СОВЕТ 64: **УЧЕБА ПОД ЗАЩИТОЙ**

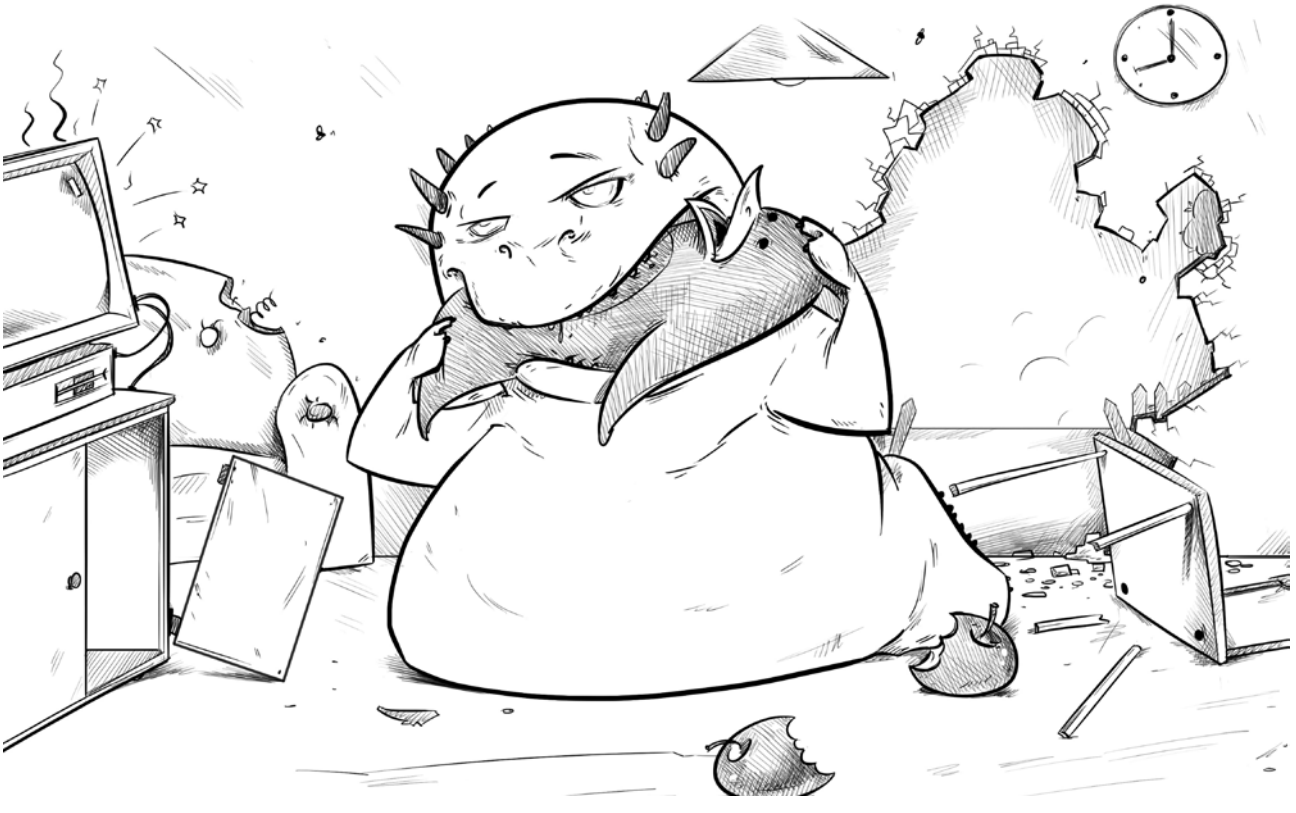
Когда юный Михаил Ломоносов шел через всю Россию учиться наукам, для защиты от лихих людей ему пришлось присоединиться к рыбному обозу. Прошло 300 лет, путь к знаниям стал легче и проще, но едва ли безопаснее. Интернет быстро снабдит пытливый ум любой необходимой информацией, но обитающие там киберугрозы попутно причинят немало неприятностей. Нежелательная реклама, кража персональной информации, шифрование содержимого жесткого диска с последующим вымогательством — лишь малая толика того, от чего можно пострадать, беспечно бороздя просторы интернета. Обеспечьте защиту детского компьютера, благо современные антивирусы рыбой практически не пахнут.

НЕ ОСТАВЛЯЙТЕ РЕБЕНКА НАЕДИНЕ С КОМПЬЮТЕРОМ

# СОВЕТ 65: **ДЕТСКАЯ ЛЮБОЗНАТЕЛЬНОСТЬ**

Дети очень любопытны, а потому такая многофункциональная штука, как компьютер, им весьма и весьма интересна (почти так же, как ваши автомобиль и ружье, но доступ к ним вы наверняка ограничили). Хорошо еще, что с его помощью малыш никого убить не сможет, а вот сам ноутбук может пострадать, причем очень быстро и очень фатально. Отдайте, наконец, ребенку его радиоуправляемую машинку, которую две недели назад взяли «на пару минут погонять», и заберите у него ноутбук.

КСТАТИ, АНТИВИРУС НУЖЕН НЕ ТОЛЬКО WINDOWS-ПОЛЬЗОВАТЕЛЯМ



# СОВЕТ 66: **УГРОЗЫ ДЛЯ ВСЕХ СИСТЕМ**

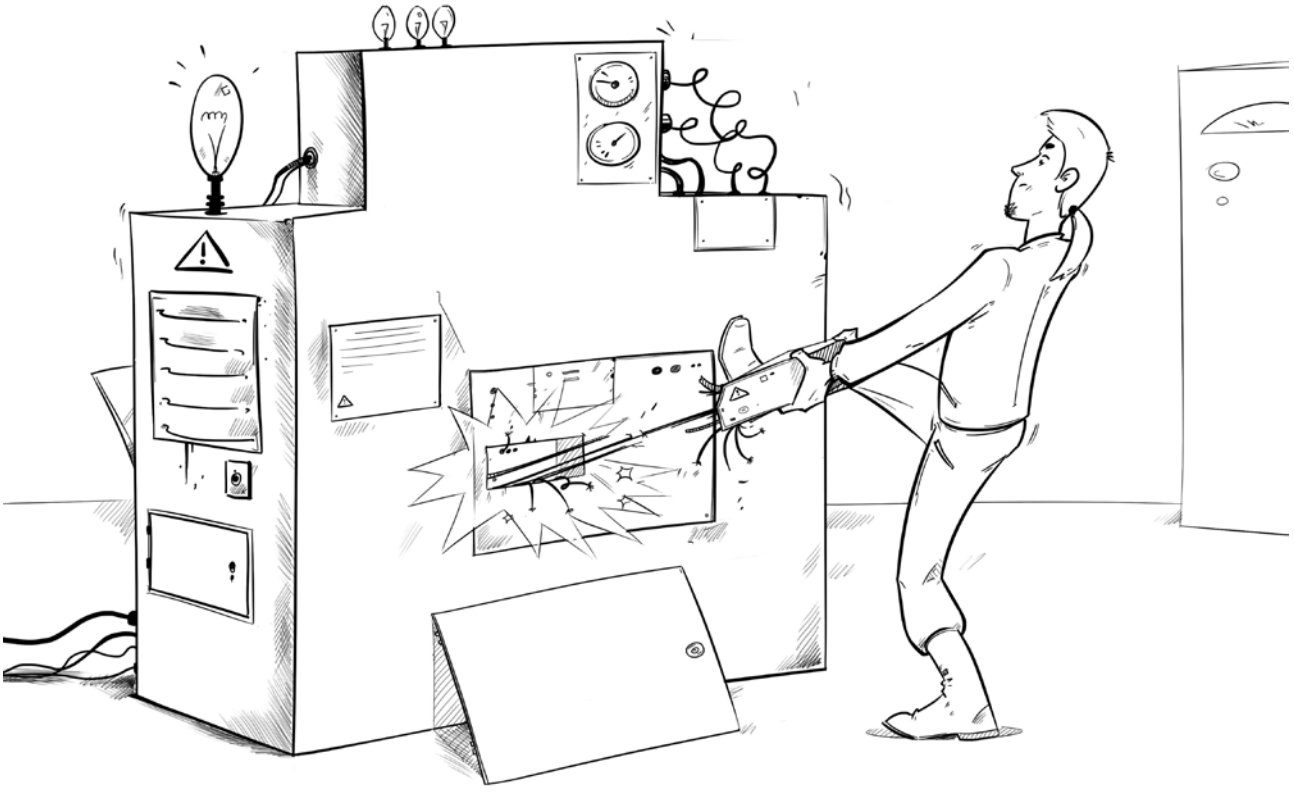
Бытует мнение, что вредоносные программы пишутся лишь под Windows, другие же платформы от этой напасти избавлены. Это верно лишь для тех операционных систем, которые, как неуловимый Джо из известного анекдота, никому не нужны. Linux и Mac OS уже давно к таковым не относятся — они достаточно широко распространены, а кроме того, их пользователи зачастую пренебрегают антивирусным ПО и другими мерами защиты, что делает их легкой мишенью. Увы, как бы ни было мало вредоносных программ для вашей операционной системы, для нарушения ее работы и кражи ценной информации хватит даже одного зловреда.


ОТКЛЮЧИТЕ АВТОЗАПУСК ФЛЕШЕК
95%
16 GB

# СОВЕТ 67: **ОПАСНЫЕ ФЛЕШКИ**

Мы учим собак ничего не подбирать с земли, чтобы они не отравились или не подавились чем-то неподходящим. Примерно то же самое владелец компьютера должен сделать для своего электронного питомца. Функция автоматического запуска файлов, расположенных на флешке или DVD-диске, будет способствовать заражению компьютера, если среди этих файлов затесалось вредоносное программное обеспечение. К счастью, в новых версиях Windows эта функция по умолчанию отключена, но если вы до сих пор пользуетесь Windows XP, стоит отучить систему от этой вредной привычки.

ИЗВЛЕКАЙТЕ УСТРОЙСТВА БЕЗОПАСНО



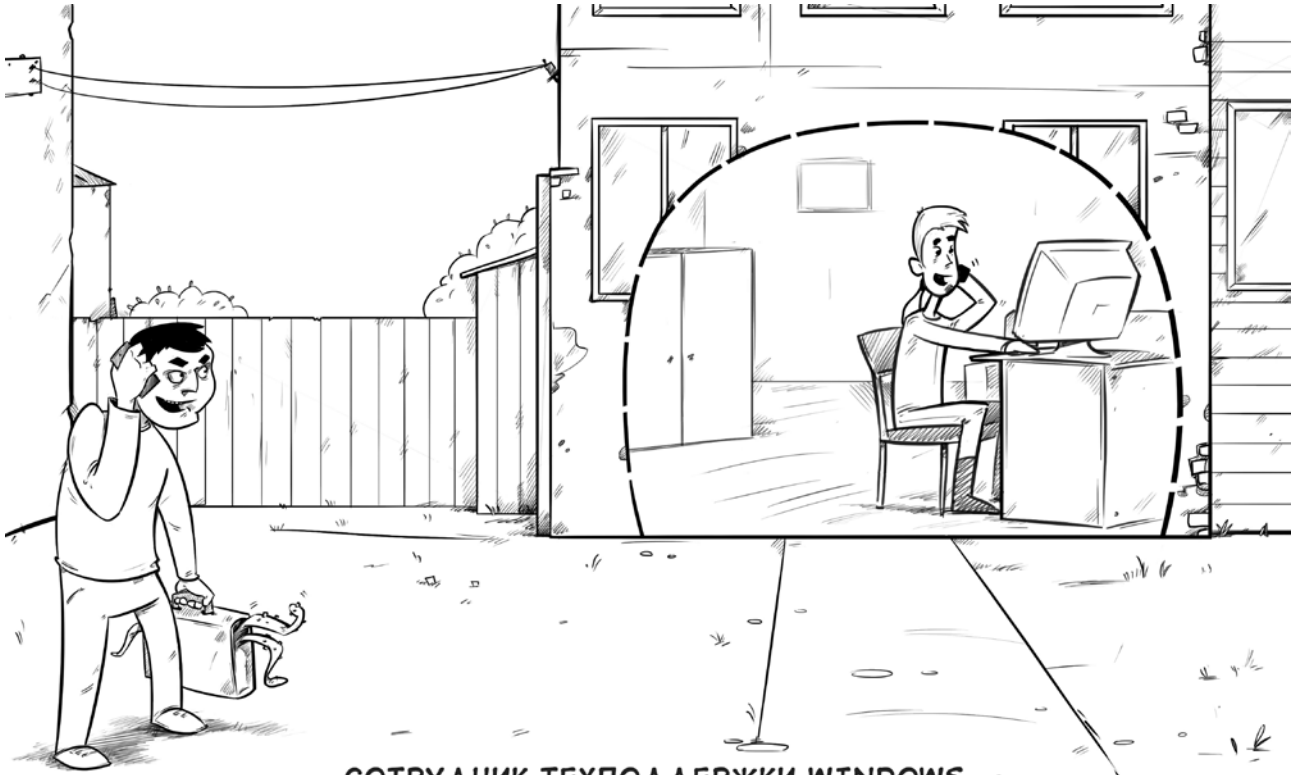
# СОВЕТ 68: **СОХРАНЕНИЕ ДАННЫХ**

Кинули файлы на флешку и выдернули ее из компа? Готовьтесь к тому, что их там не окажется. Нет, это не диверсия. Как ни странно, это сделано для удобства пользователей. Дело в том, что флешка записывает данные гораздо медленнее, чем компьютер их может передать. Поэтому, чтобы не тратить много времени на процесс передачи, Windows записывает передаваемые данные в специальную область памяти (буфер), из которой они постепенно сбрасываются на флешку. После записи в буфер последней порции информации Windows убирает с экрана окно с индикатором прогресса копирования файлов, но это совсем не значит, что запись уже завершена. Если флешку надо выдернуть срочно, поможет функция безопасного извлечения устройства, после ее использования запись гарантированно завершится.

ВЕБ-КАМЕРА МОЖЕТ ИСПОЛЬЗОВАТЬСЯ ДЛЯ ШПИОНАЖА

# СОВЕТ 69: **НЕЗАМЕТНЫЙ ШПИОН**

Веб-камера — величайшее изобретение, прежде всего для тех, чьи друзья или родственники находятся за тридевять земель. Но не все так позитивно, поэтому примите меры, чтобы камеры ваших устройств не могли выдать злоумышленникам подробности вашей личной жизни. Использовать их можно по-всякому, в зависимости от фантазии хакера и от сюжетов, которые ему удалось заснять: начиная от продажи фото и видео на порносайты и заканчивая шантажом запечатленных героев. Не хотите попасть в неприятную ситуацию — пользуйтесь защитными средствами, благо контролировать доступ к веб-камерам современные антивирусы уже научились.



СОТРУДНИК ТЕХПОДДЕРЖКИ WINDOWS —
ПОПУЛЯРНЫЙ У МОШЕННИКОВ ОБРАЗ

# СОВЕТ 70: **ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО**

«Здравствуйте, я сотрудник техподдержки Windows, на вашем компьютере обнаружен особо опасный вирус», — так может начинаться разговор с телефонным мошенником. Схема обмана проста: злоумышленник убеждает пользователя, что его компьютер заражен, и просит проделать на компьютере ряд действий, которые якобы избавят его от заразы. Но на самом деле выполнение команд мошенника и приводит к появлению на компьютере вредоносной программы. Потому стоит запомнить: сколько бы вирусов ни было на вашем компьютере, из Microsoft вам не позвонят.

Если вы внимательно прочитали наши советы, значит, вы предупреждены и можете встречать информационные угрозы лицом к лицу и с поднятым забралом. Но для полной уверенности в собственной безопасности стоит стать еще и вооруженным, установив антивирусное программное обеспечение – например, наш Kaspersky Total Security, пробную версию которого можно загрузить со страницы https://survival.kaspersky.ru

Информацию о новых мошеннических рассылках, актуальных операциях киберпреступников, местах обитания вирусов и выпаса троянских коней ищите в нашем блоге https://blog.kaspersky.ru