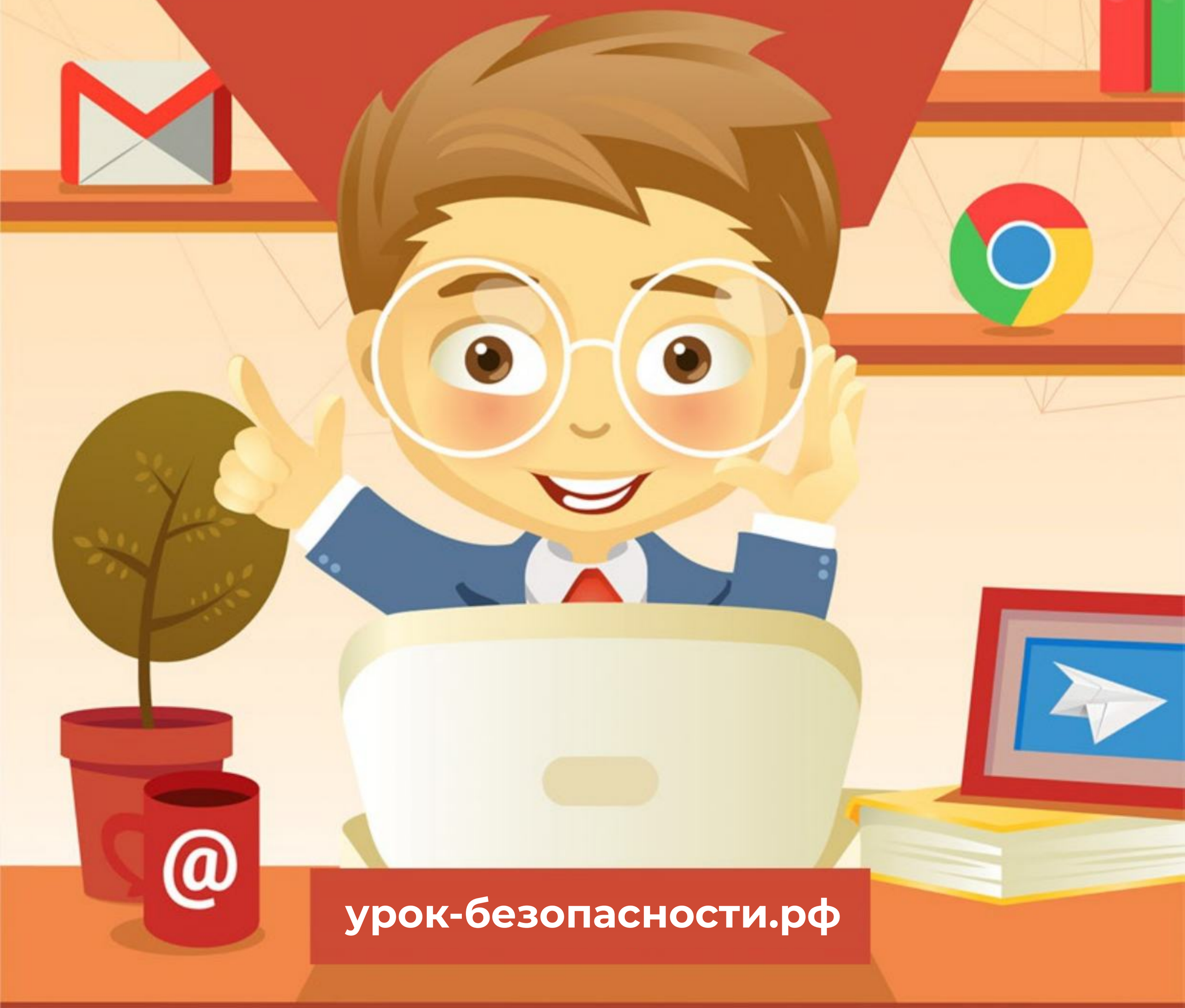
ПРАВИЛА БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ



урок-безопасности.рф

Правило № 1.
Не открывайте в Интернете незнакомые сайты и не скачивайте подозрительные файлы

1. Если вы зашли на малознакомый сайт и при этом вам что-то показалось в нем подозрительным, лучше будет закрыть подобный ресурс, нажав на крестик на его вкладке (обычно располагается справа, обозначается X).

2. Если незнакомый сайт предлагает вам скачать какую-либо непонятную программу, откажитесь от скачивания – **это может быть вирус**.

3. Перед началом работы в Интернете потребуется **работающая антивирусная программа** – она предотвратит возможное выполнение зловредных программ и будет регулярно проверять компьютер на наличие вирусов.

4. Если вы раздумывайте о том, стоит ли перейти по непонятной ссылке или загрузить непонятную программу, лучше откажитесь от этого – именно на это рассчитаны вредоносные приложения, программы-вирусы или опасные сайты, которые заражают ваш компьютер.

ЖМИ

Загружайте файлы только с доверенных сайтов.

Правило № 2.
Защита почты от нежелательных писем (спама).

Спам (SPAM) -это письма, которые приходят на вашу электронную почту от рекламодателей или людей, которых вы не знаете (зачастую мошенников).

Вполне возможно, что в этих письмах содержатся вирусы или иные вредоносные вложения, а также ссылки. Кроме того, в таком письме вас могут попросить перейти на сайты, где потребуется написать пароль от вашей почты или данные банковской карты.

Если вам пишут, что вы внезапно выиграли 10 миллионов долларов, стали призером лотереи или предлагают быстро разбогатеть, заработать большие деньги буквально за 15 минут работы в день – это обман!

1. Письма от людей, сервисов и компаний, которые вам неизвестны, **следует сразу удалить**, не читая.

2. **Не верьте рекламе**, которая обещает выгодный отдых за границей, неожиданный суперприз или очень дешевый автомобиль. Любое неправдоподобно выгодное предложение – 100%-й способ обмануть доверчивых пользователей.

Правило № 3.

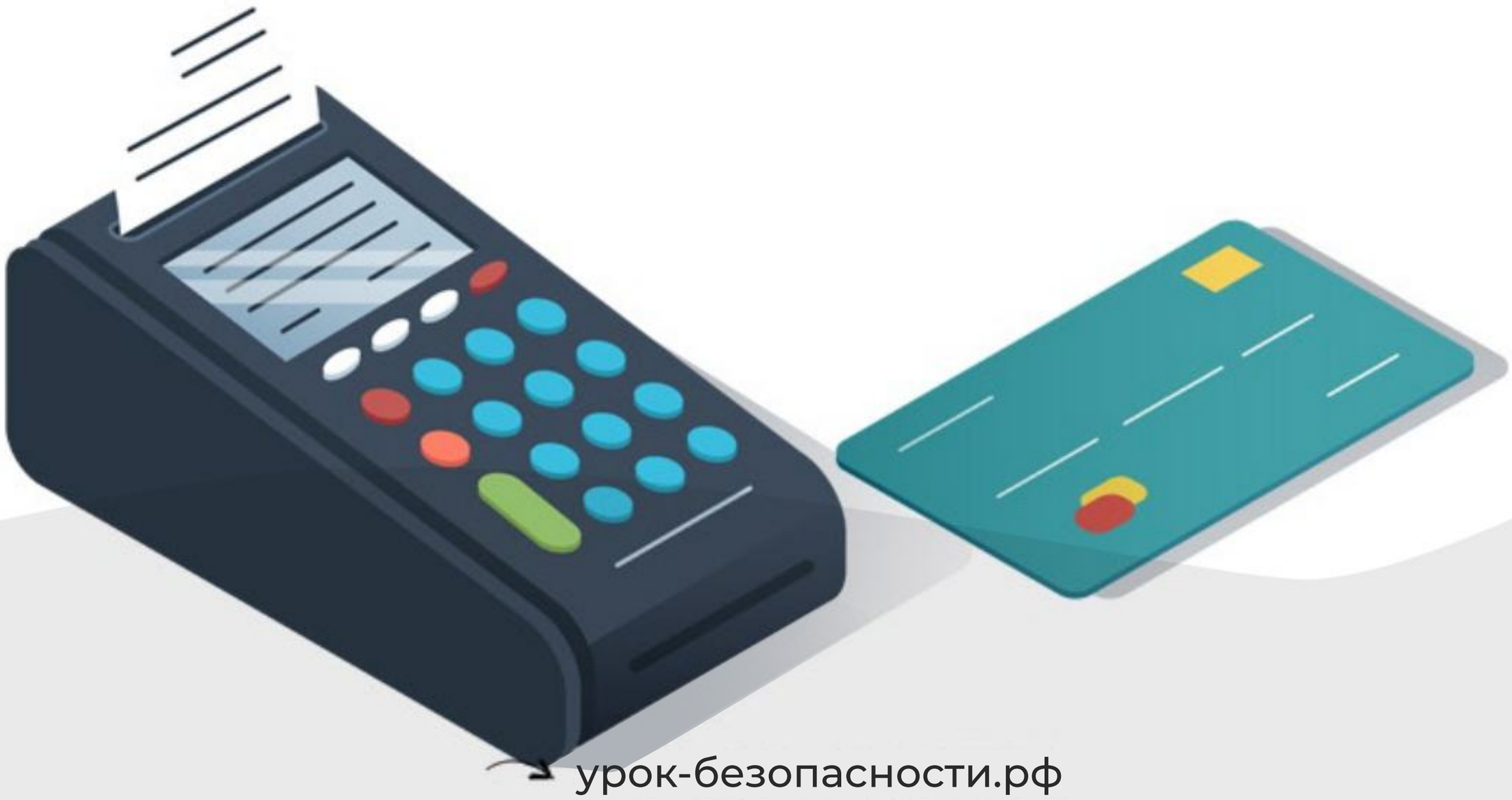
При покупке товаров в интернет-магазинах соблюдайте осторожность.

1. При покупке товаров в интернет-магазинах или прочих сервисах проверяйте незнакомые сайты, особенно, если вы приобретаете что-то на них впервые.
Одно из лучших средств – наличие отзывов о магазине или сервисе.

2. Сравнивайте цены на товары в разных магазинах.
Постарайтесь узнать о магазине и о товаре побольше.

3. Обязательно изучите правила доставки, покупки, информацию по гарантии, возврату товара и т. п., уточните, предоставляет ли продавец кассовый чек.

4. Обязательно запомните, что ни интернет-магазин, ни банк никогда не будут просить указать PIN-код вашей банковской карты или пароль от любого личного кабинета – это делают лишь мошенники!



Правило № 4.

Поменьше своих реальных данных в Интернете.

Злоумышленникам может хватить даже незначительных сведений – скажем, места учебы, названия спортивной команды и т.п. – для осуществления противоправных действий.

Вы ведь не будете случайному дяде и тете в торговом центре сообщать о себе данные, если они попросят, верно? В Интернете этого не следует делать тем более.

В Сети достаточно зловредных ресурсов, которые будут настойчиво просить вас написать о себе достоверную информацию для «бесплатных подарков» или прочих заманчивых вещей. Практически всегда ваши данные в таком случае будут использовать во вред вам же.

1. Ни в коем случае в Интернете не оставляйте незнакомым сайтам, сервисам и людям номера телефонов, место учебы, адрес и ФИО, данные своих друзей и близких.

2. Ни в коем случае не рассылайте свои фотографии незнакомым лицам – только с разрешения родителей!

Правило № 5.
Установите антивирусную защиту

на компьютер и регулярно обновляйте антивирусную программу и ее базы.

Вирусы или другие зловредные программы способны атаковать любой компьютер – от обычного сбора статистики до кражи средств с карты или удаления всех данных на компьютере. Помните, что размещение вирусов под видом «полезных» или «необходимых» программ – излюбленное средство мошенников.

Для противодействия вирусам используется эффективное средство – антивирус.

Установите антивирус на свой компьютер, не забывайте регулярно обновлять антивирусную программу и ее базы.

1. Если установленный антивирус считает сайт, на который вы хотите перейти, подозрительным – лучше не рисковать и прислушаться к совету программы.

2. Не скачивайте непонятные/неизвестные файлы и программы из Интернета себе на компьютер.

3. Каждый скачанный файл проверьте антивирусной программой на наличие вирусов.

Если уж вы скачали подобный файл/ программу, не открывайте его, а постарайтесь побыстрее удалить.

Правило № 6.
Создавайте надежный пароль

для личного почтового ящика или при регистрации на сайтах. Так вы обезопасите себя от мошенников и потери личной и важной информации.

*****

1. Пароль должен содержать *БУКВЫ И ЦИФРЫ*.

2. Используйте РАЗНЫЕ ПАРОЛИ ДЛЯ РАЗНЫХ САЙТОВ, а не один для всех.

3. В качестве пароля можно придумать СЛОВОСОЧЕТАНИЕ.

   Например, «Мой друг Саша бегает 2 раза в неделю» и составить пароль из первых букв каждого слова, написав их латиницей, а также добавив цифру. В результате получится «MdSb2rvn». Это надежный пароль.

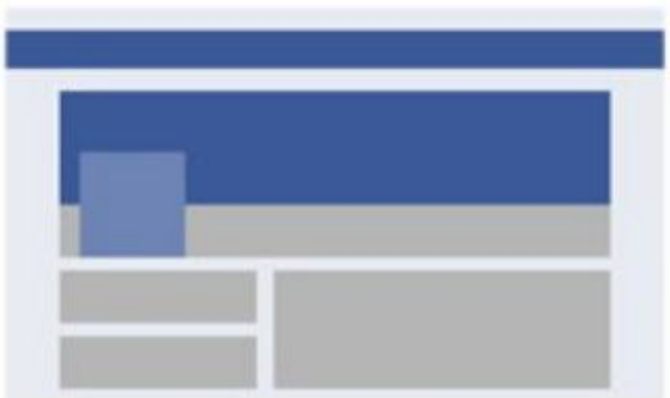
4. Не забывайте записывать пароли и хранить их в НАДЕЖНОМ МЕСТЕ.

5. НЕ ГОВОРИТЕ ваш пароль незнакомым людям.

Правило № 7.
Не переходите по подозрительным ссылкам

Очень часто среди мошенников применяется технология **фишинга** (phishing/fishing – «рыбалка», «выуживание»).

В поддельное электронное письмо (которое часто может казаться важным) вставляется ссылка, которая якобы ведет на общеизвестный сайт.



Нажимая на нее, пользователь попадает на вредоносный ресурс, зачастую с виду неотличимый от оригинального.

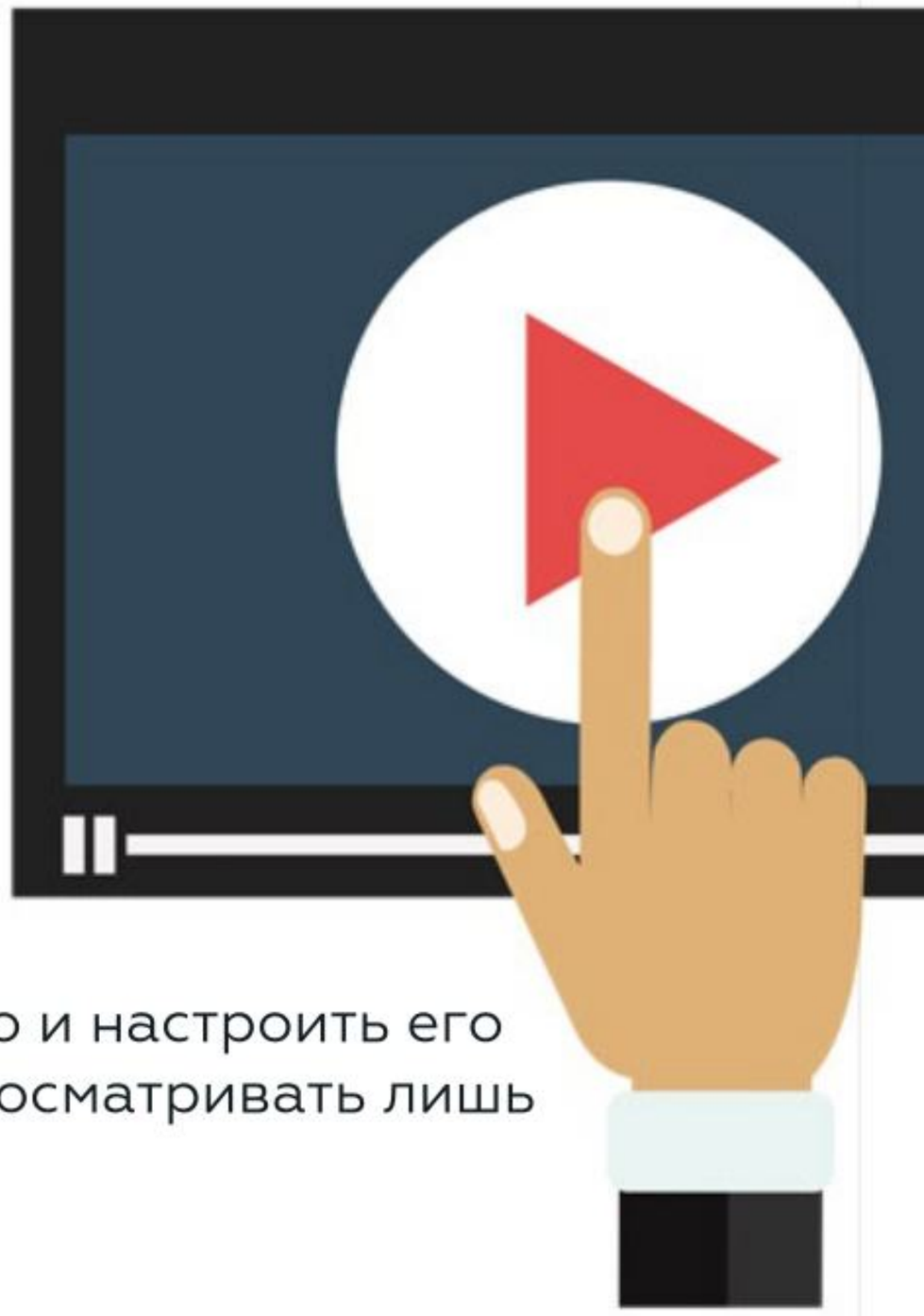
Далее пользователь вводит свои учетную запись и пароль (в некоторых случаях дело доходит и до данных банковских карт и прочей персональной информации), в результате чего конфиденциальные данные перехватываются злоумышленниками.

Часто подростки пользуются программами быстрых сообщений: Skype, ICQ и др., а также социальными сетями. Ссылка на мошеннический сайт может быть прислана и через них (например, от взломанных учетных записей ваших знакомых и друзей). В таком сообщении может содержаться просьба проголосовать за какую-либо фотографию или видеоролик.

Проголосуй за меня

Правило № 8. Используйте YouTube в режиме безопасности

У популярного ресурса YouTube есть **режим безопасности**, в котором не отображаются материалы для взрослых и информация по ограничению возраста.



Иначе говоря, безопасный режим популярного сервиса старается сделать все, чтобы скрыть нежелательное содержимое, при этом не удаляя никакие материалы.

На сервис можно загрузить собственное видео и настроить его просмотр таким образом, чтобы его смогли просматривать лишь определенные пользователи.

1. Выберите при загрузке ролика опцию «Не в списке» или «Личное», чтобы ваше видео было доступно только тем, кому вы доверяете.

2. **Не загружайте на YouTube содержимое**, которое может потенциально навредить вам или вашим близким в будущем.

Правило № 9.
Не открывайте почтовые сообщение от неизвестных источников

Любой электронный почтовый ящик может быть настроен так, чтобы избегать получения писем, пришедших с определенных адресов или согласно некоторым правилам.

Фильтры электронной почты следует настроить так, чтобы блокировать поток нежелательных писем (спама).

Ни в коем случае **не открывайте письма от незнакомых людей, компаний, сервисов**, а если уж открыли, то не открывайте вложенные в них файлы, не переходите по содержащимся в них ссылках.

В противном случае вы рискуете стать жертвой фишинга или попытки загрузки на ваш компьютер вредоносной программы.

Именно поэтому первой линией обороны должны являться вы сами: **вложения или переход по ссылке можно открывать только от тех отправителей, в которых вы точно уверены.**

Правило № 10.
Не общайтесь в Интернете с незнакомыми людьми

Средств для общения в Интернете хватает: всевозможные мессенджеры, почтовые программы, онлайн-чаты в браузерах, социальные сети, онлайн-игры и т. д.

Если через любое из этих средств общения вы начали получать нежелательные, неприятные или странные сообщения от подозрительных личностей, следует прекратить контакты с подобными собеседниками.

Вопросы, задаваемые ими, могут касаться личной жизни или деятельности ваших друзей/близких. В подавляющем большинстве случаев это злоумышленники, стремящиеся выудить у вас побольше информации, чтобы получить доступ к персональным данным.

Ни в коем случае не соглашайтесь на встречу с такими людьми, что бы они ни обещали, как бы себя ни называли или запугивали вас.

Правило № 11.
В Интернете будьте дружелюбны и естественны

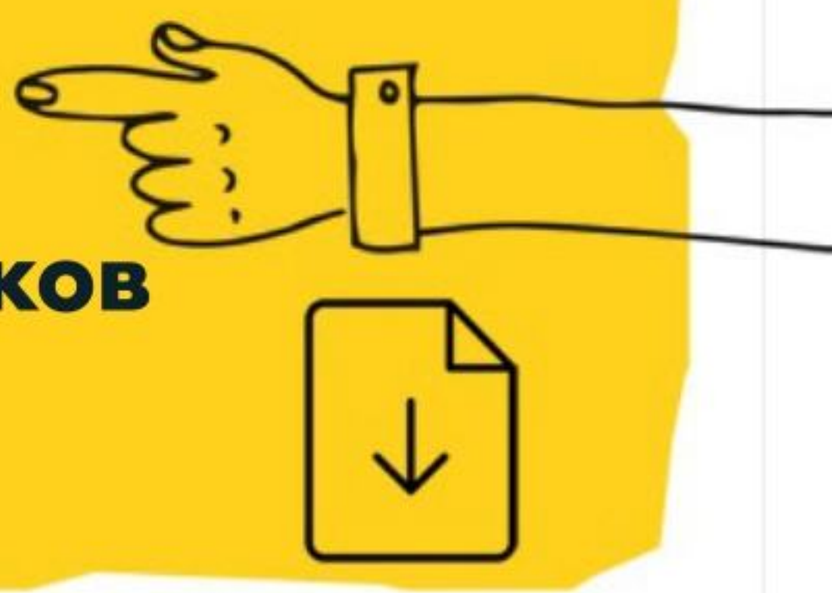
Общение в Интернете вовсе не подразумевает того, что вы можете безнаказанно казаться кем-то другим.

Ваша реальная личность все равно себя со временем проявит (это подтвердит любой психолог), поэтому постарайтесь никому не грубить, не высказывать резких слов, не издеваться и не лгать. Просто ведите себя как благоразумный человек.

Помните, **что все противозаконные действия и негативные высказывания в Интернете подразумевают такую же ответственность, как и в реальном мире!**

Поставьте себя на место других людей – вы сразу поймете, как неприятно читать хамство, грубости или пугаться серьезных угроз от незнакомых личностей.

Правило № 12. Скачивайте информацию только из проверенных источников



В электронных письмах, программах быстрых сообщения (ICQ, Skype и т.п.) есть возможность пересылки друг другу файлов. Старайтесь не принимать файлы от незнакомых источников, как бы они не именовались и что бы отправитель вам ни говорил.

Часто злоумышленники вкладывают в письма или рассылают через мессенджеры архивы.

- Если вы незнакомы с отправителем, лучше такой файл не скачивать.
- Если вы по неосторожности все-таки скачали его, обязательно проверьте его после этого антивирусной программой.

Даже скачанная программа не сможет причинить вам ущерба до тех пор, пока вы не попытаетесь ее открыть (например, архив ZIP) или запустить (например, файл формата EXE).

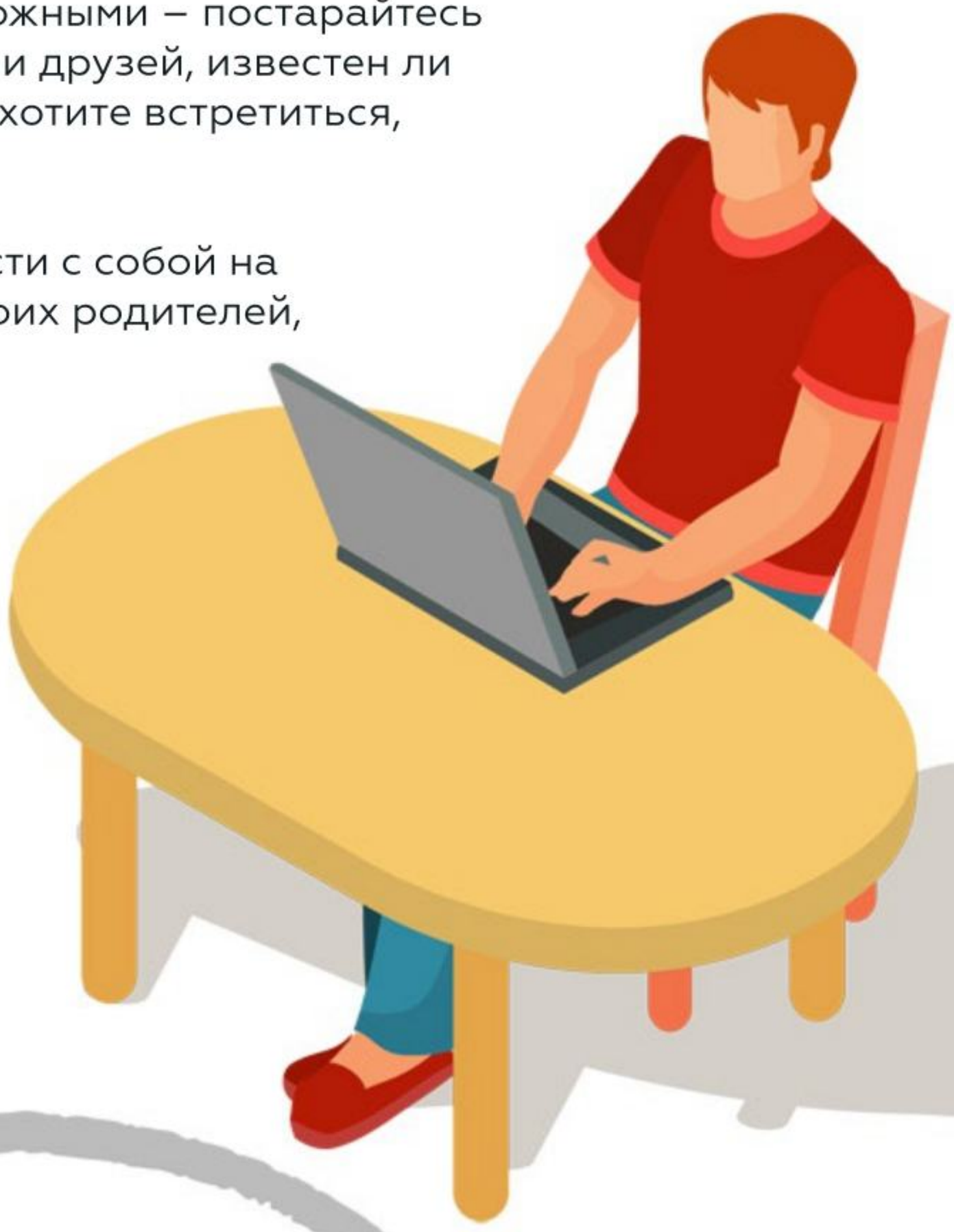
Необходимые для учебы или иной деятельности программы лучше скачивать с официального сайта разработчиков, а не с файлообменников – это гарантия того, что вы не занесете при скачивании на ваш компьютер вирус и получите последнюю версию нужной программы.

Правило № 13.
Будьте предельно внимательны при реальной встрече с интернет-другом.

Перед тем, как встретиться с кем-либо в реальной жизни, не бойтесь показаться осторожными – постарайтесь расспросить своих знакомых и друзей, известен ли им тот человек, с которым вы хотите встретиться, что они о нем говорят.

Совсем неплохо будет привести с собой на первую реальную встречу своих родителей, стесняться этого не следует. Нового знакомого также попросите привести с собой своих родных.

Если в какой-то момент времени вы понимаете, что общение с новым «другом» заходит в тупик или идет по непонятному для вас сценарию, лучшим решением будет прекратить общения с таким человеком навсегда.



Не забывайте, что реальный мир – это все же не виртуальное общение, здесь все недостатки и достоинства человека (физические и психологические) выглядят иначе. Это следует учитывать во время реальной встречи.

Правило № 14.
Не шлите SMS-сообщения на незнакомые номера телефонов

Чрезвычайно популярной схемой мошенничества в Интернете является просьба отослать SMS-сообщение на некоторый номер, после чего вы якобы получите доступ к желаемому содержимому.

Кроме отсылки SMS, хакеры могут попросить выслать и иную информацию – не говоря уже о том, что почти наверняка с баланса снимут большие деньги.

Не поленитесь и поищите номер, на который просят отправить SMS, в обычном поисковике. Зачастую на первых же страницах поиска вы увидите сообщения от обманутых пользователей вроде: «Обманщики!», «Ничего не отсылайте!», «Развод конкретный» и т. п.

Также проверьте подобный телефон на специализированном сайте. Кроме того, следует поискать отзывы о сервисе, который просит отсылать подобные SMS-сообщения.