Центр мониторинга социальных сетей

БУДЬ В БЕЗОПАСНОСТИ: КАК НЕ СТАТЬ ЖЕРТВОЙ IT-ПРЕСТУПЛЕНИЙ

ТОП-10 ПРАВИЛ

Появление в нашей повседневной жизни современных компьютерных устройств и программных сервисов делает нашу жизнь намного удобнее, но требует определённых навыков и знаний.

Одновременно с развитием таких устройств появляются виды мошенничества, позволяющие нас обмануть и присвоить наши денежные средства.

Чтобы не стать жертвой преступников, обезопасить себя и своих близких от посягательств на их персональные данные и личные сбережения, необходимо придерживаться соблюдения ключевых правил медиабезопасности.

1

Не добавляйте незнакомых людей в друзья

Одно из ключевых правил безопасности гласит - никогда не говорите на улице с незнакомцами. Это же правило действует и в Интернете.

Только здесь притворяться другим человеком гораздо проще, чем в реальной жизни. Просто знайте, что за аватаркой симпатичной девушки может скрываться кто угодно – особенно если она отчаянно пытается узнать адрес или, например, модель компьютера.

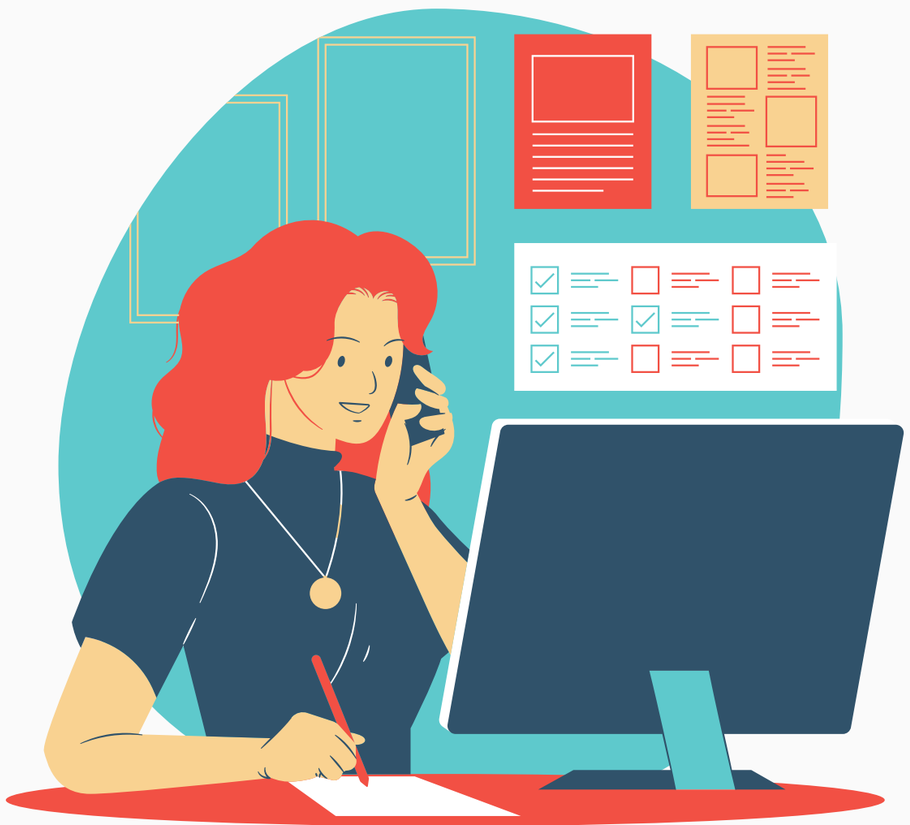
2

Никому не сообщайте личную информацию

Никогда и ни при каких обстоятельствах нельзя сообщать информацию личного характера, в том числе свои персональные данные, к которым относятся: фамилия, имя, отчество, дата рождения, домашний адрес, номера телефона, банковских карточек, пароли.

Знакомясь и общаясь в Интернете, обращайте внимание на вопросы, которые вам задают новые друзья.

В случае подозрения виртуальных друзей в попытках обмана — немедленно прекращайте общение!

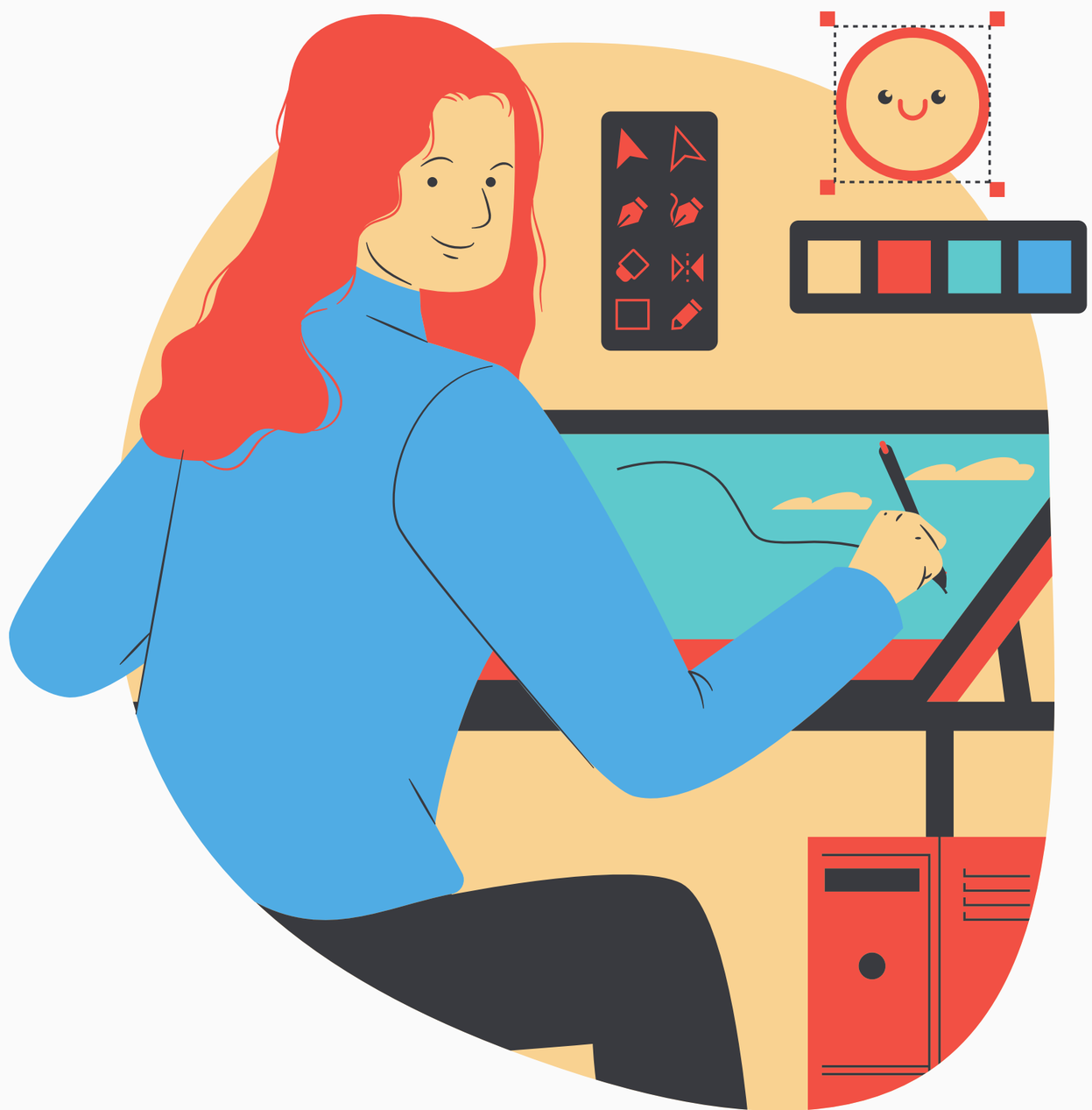


3

Не скачивайте программы с сомнительных сайтов

Используйте для загрузки приложений только официальные Интернет-ресурсы.

Скачав программу с первого попавшегося ресурса, можно легко поймать вирус, из-за которого не только сломается техника, но и у злоумышленников окажутся номера как ваших банковских карт, так и ваших родителей.

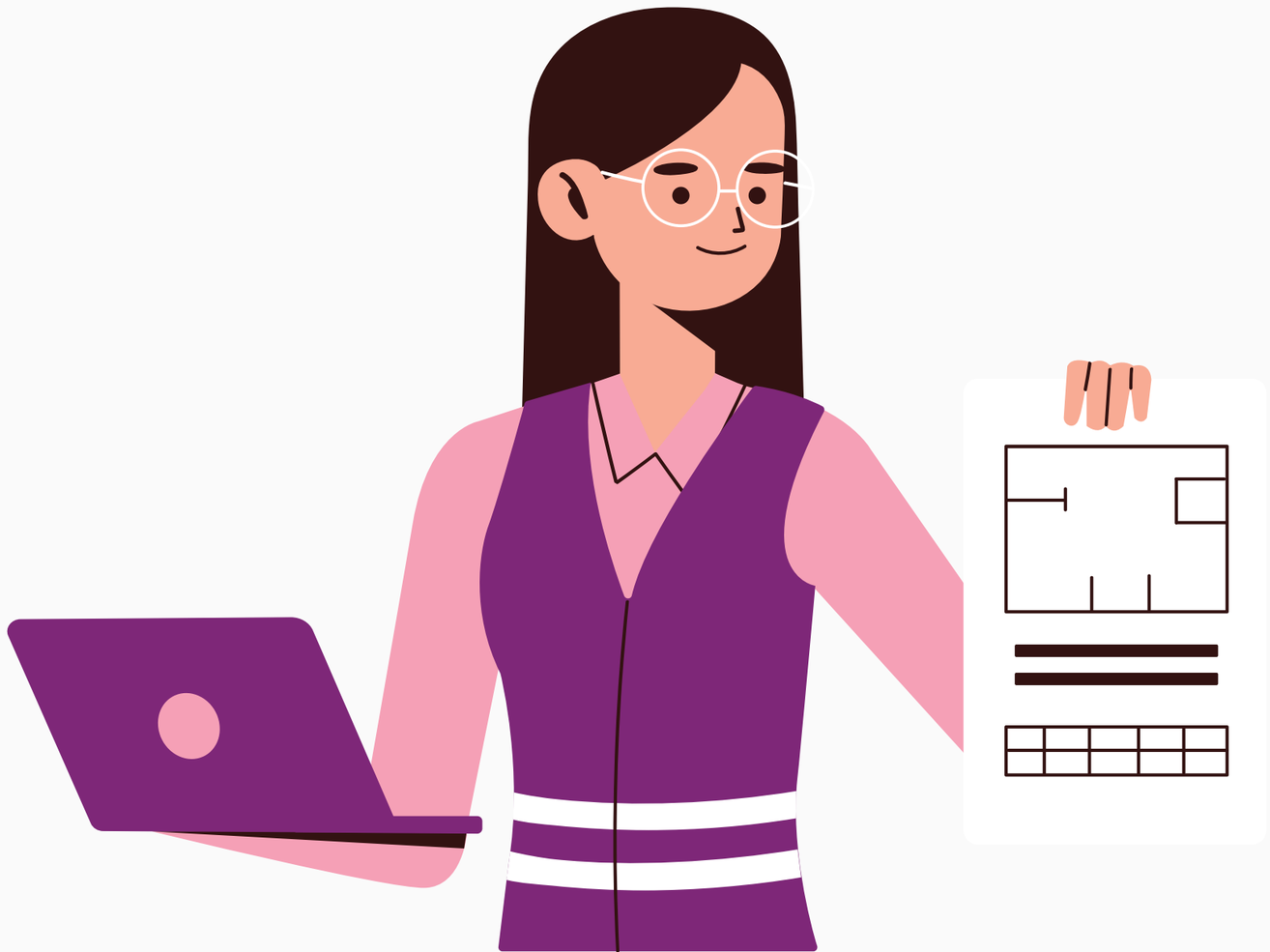


4

Не переходите по подозрительным ссылкам

Нельзя нажимать на подозрительные ссылки, которые приходят по электронной почте или в сообщениях.

Например: «*Посмотри, что здесь о тебе говорят*», «*Ты стал обладателем нового* iPhone*— переходи по ссылке, чтобы забрать его*». Нужно знать, что такие сообщения отправляют мошенники и при переходе по данной ссылке есть большой риск того, что на ваш компьютер или смартфон попадёт опасный вирус.



5

Не ставьте геометки под фото

По ним злоумышленники легко узнают, где вы живёте и учитесь. Конечно, нет ничего страшного в том, что вы проставите геометку на фотографии, например, со школьной экскурсии. Но табу должны стать личный адрес, адрес вашего образовательного учреждения и работы близких друзей или родственников.

6

Перепроверяйте сообщения с просьбами о помощи от друзей и родственников

Иногда мошенники взламывают аккаунты в соцсетях и рассылают всем друзьям сообщения с просьбой перевести деньги. Не торопитесь с помощью, свяжитесь по телефону с человеком, со странички которого пришло сообщение, чтобы самому узнать, нужны другу деньги или нет. Или посоветуйтесь с родителями.

7

Не переходите на подозрительные страницы для совершения онлайн-покупок

Мошенники любят совершать онлайн-покупки не меньше, чем вы, но у них на это есть свои причины. В виртуальном мире бдительность ослабевает, и игроки могут не заметить обмана.

Покупателей заманивают низкими ценами и «уникальными акциями». И не стоит заблуждаться, в подобные ловушки могут попасть не только дети, но и взрослые.

Прежде чем вводить на странице сайта свои персональные данные, пароли, коды или реквизиты банковской карты для совершения покупки —- удостоверьтесь, что это не мошенническая страница.

Платежи в интернете нужно согласовывать со взрослыми. И лучше подключить уведомления о платежах!

8

Не надейтесь на быстрое обогащение

Если вам не хватает карманных денег на модный телефон и терпения, чтобы на него накопить, мошенники с радостью вам «помогут»! Они размещают в интернете множество объявлений о быстром и легком заработке. Но зачастую в таких случаях внезапно разбогатеть удается только самим махинаторам.

Мошенники могут убедить вас вложить деньги в «сверхприбыльный проект» (спойлер — в финансовую пирамиду). До выплат вкладчикам дело обычно не доходит. Собрав деньги с как можно большего числа людей, организаторы исчезают.

Порой обманщики предлагают «быстро заработать», просто зарегистрировавшись на сомнительном сайте. Надо только выполнять задания или делать букмекерские ставки. Для вывода «заработка» они просят оплатить комиссию. В итоге деньги вместе с данными карты оказываются в руках махинаторов.

9

Не верьте в легкие «выигрыши» в конкурсах

Нередко мошенники рассылают письма и сообщения, в которых обещают нежданный выигрыш или от имени популярных блогеров запускают рекламу «беспроигрышных лотерей». Но затем за доставку «приза» или какие-то другие дополнительные услуги просят оплатить небольшую комиссию. Для этого надо пройти по ссылке и ввести данные банковской карты. Но на самом деле ссылка ведет на фишинговый сайт, и вместо призов доверчивый пользователь получает убытки.

Если организаторы конкурса просят что-либо оплатить, это повод насторожиться. Прежде чем пытать удачу в онлайн-розыгрышах, надо убедиться, что организаторы — не мошенники: почитать отзывы в интернете, новости (вдруг они уже замечены в скандалах). Стоит проверить на официальной странице блогера, действительно ли он рекламирует этот конкурс, или он тоже стал жертвой мошенников.

10

Не используйте найденную банковскую карту на улице

Если вы нашли банковскую карту, то в соответствии со статьей 227 ГК РФ, Вы обязаны немедленно уведомить о находке лицо, потерявшее ее, и возвратить найденную вещь этому лицу. Если же владелец пластиковой карты вам не известен, вы должны заявить о находке в полицию или отделение банка.

При попытке оплатить что-нибудь в интернете, пароль придёт на номер телефона держателя. Почти везде предусмотрена двухфакторная аутентификация.

При попытке снять наличные вы попадёте на камеры видеонаблюдения, которыми оборудованы банкоматы.

За попытку взлома чужого счёта предусматривается штраф до 120 000 рублей, обязательные или исправительные работы либо лишение свободы до трех лет. Также уголовное дело может быть возбуждено за кражу.

Контакты

В случае, если вы или ваши близкие стали жертвой преступления, в обязательном порядке необходимо обращаться в полицию по телефону 112 или 02.