Волго-Донская транспортная прокуратура разъясняет

«Безопасность в сфере использования информационно-коммуникационных технологий»

Установите антивирусные программы

Вирус – это вредоносная программа, которая проникает на ваш компьютер, ноутбук или смартфон различными способами. Она способна не только помешать работе, например, сделать недоступной часть постоянной памяти, но и похитить конфиденциальную информацию: логины, пароли, банковские реквизиты. Для защиты от вирусов существуют антивирусы. Важно не просто пользоваться ими, но и периодически обновлять их базы данных, ведь создатели вредоносных программ то и дело запускают в интернет свои новые разработки.

Используйте сложные логины и пароли

Хороший логин и пароль – это сложная комбинация, в которой используются заглавные и строчные буквы, цифры и символы. Лучше задействовать специальные программы, которые генерируют их, запоминают и надежно хранят. И желательно пользоваться разными сочетаниями логинов и паролей для разных сайтов.

«Разлогинивайтесь» на чужих устройствах

Воспользовались чужим компьютером? После этого недостаточно просто закрыть страницу, на которую вы заходили. Не забывайте предварительно выходить из всех аккаунтов, соцсетей и мессенджеров на устройстве. В противном случае человек, который сядет за этот компьютер после вас, получит возможность войти в вашу учетную запись и сделать с ней все, что ему заблагорассудится.

Проверяйте безопасность соединений

Всегда обращайте внимание на то, что написано в адресной строке. Если вы видите, что адрес сайта начинается с HTTPS – все в порядке, это безопасное соединение и здесь можно вводить конфиденциальную информацию. Если же адрес начинается с HTTP – это значит,

что соединение не защищено. Также слева от HTTPS должен быть значок в виде замка. Для большей уверенности в безопасности соединения можно кликнуть на него и просмотреть информацию во всплывающем окне.

Будьте внимательны к соединениям Wi-Fi

Общедоступные соединения есть, например, в кафе, торговых центрах и аэропортах. Не используйте их, если собираетесь вводить логины, пароли, либо совершать оплату услуг и товаров через интернет. Либо вообще не пользуйтесь ими ни при каких обстоятельствах и ограничьтесь обычным мобильным интернетом.

Создайте две почты – для работы и личную, ограничьте информацию о себе в интернете

Лучше не выкладывать на всеобщее обозрение свой номер телефона, адрес электронной почты и другую контактную информацию. Если это нужно сделать в связи с должностными обязанностями или поиском работы, создайте адрес электронной почты и номер телефона, которые будут использоваться только для этого. Многие социальные сети позволяют настраивать список тех, кто может просматривать ваш профиль и отправлять сообщения. Можно, например, сделать так, чтобы писать вам было разрешено только тем, с кем у вас подтверждена дружба – и при этом, конечно, стоит убедиться, что вы имеете представление о каждом своем онлайн-друге.

Не передавайте конфиденциальные сведения и не храните сканы документов

Не пересылайте пароли, логины, сканы и фотографии документов, ПИН-коды и прочую подобную информацию в мессенджерах, чатах или по электронной почте. Не делайте этого, даже если ваш собеседник утверждает, что он – представитель службы безопасности банка. Если есть сомнения, лучше перезвоните в ваш банк или иную организацию, сотрудником которой представляется человек, и уточните информацию. Если такая необходимость все же возникла, например, по работе или если нужно дистанционно направить заявление, после удалите письмо или сообщение в мессенджере. Но перед этим убедитесь, что адресат получил документы.

Не открывайте подозрительные письма

Прежде чем открыть письмо, пришедшее на электронную почту, прочитайте заголовок и посмотрите, с какого адреса оно было отправлено. Если тема вам неинтересна, заголовок составлен с грубыми ошибками, адрес представляет собой хаотичное нагромождение символов или напоминает название вашего банка, но с переставленными буквами, сразу отправляйте письмо в корзину. И никогда не открывайте файлы .exe в подозрительных письмах.

Не переходите по подозрительным ссылкам

Даже если всплывающая ссылка обещает что-то очень интересное и выгодное, лучше не кликать на нее. Если ссылку прислал вам знакомый, причем без каких-либо комментариев, сначала уточните, что он имел в виду. Возможно, его взломали, и теперь мошенники используют его профиль для рассылки вредоносных программ.

Не устанавливайте сомнительные приложения

Есть два безопасных источника приложений:

- официальные магазины, созданные Apple, Google, Microsoft и другими подобными компаниями;
- официальные сайты компаний, разработавших приложения.

Установка приложений из других источников, в том числе различных ломаных и пиратских версий, может закончиться тем, что вам придется тщательно чистить компьютер или телефон от вирусов.

И со знакомыми будьте аккуратнее

Люди и общение бывают разными. И совместные фотографии, видео, цитаты из переписок могут быть использованы против вас. Поэтому прежде чем отправить что-то личное даже хорошо знакомому человеку, подумайте, не превратится ли в последующем этот контент в компромат.

Блокируйте подозрительных пользователей

Если у вас появились подозрения, что тот, кто пишет вам в интернете – мошенник, смело блокируйте его. Это не займет много времени, но поможет сберечь нервы и денежные средства. Многие из мошенников знают, как вызвать жалость, обмануть, запугать и заговорить человека. Поэтому с такими людьми лучше даже не вести бесед и смело отправлять в черный список. Также у нас есть удобная услуга «Безопасный режим», подключив которую, нежелательные сообщения, спам и интернет-подписки будут блокироваться автоматически.

Создайте отдельную карту для платежей в интернете

Необязательно вводить данные вашей основной банковской карты в интернет-магазинах. Зарегистрируйте отдельную, с которой вы будете оплачивать все онлайн-покупки, и не храните на ней большие суммы. Если ее реквизиты как-то попадут к мошенникам, ваши финансовые потери не будут слишком серьезными.

Будьте осторожны и внимательны!