Правила информационной безопасности

Регулярно обновляйте программы и операционную систему.

Постоянное обновление гарантирует, что для защиты вашего компьютера или смартфона используются новейшие исправления безопасности.

Установите антивирус и регулярно его обновляйте.

Антивирус позволяет проверять, обнаруживать и удалять угрозы до того, как они создадут проблему. Он также помогает защитить ваш компьютер и данные от злоумышленников.

Используйте надежные пароли, которые трудно подобрать, и нигде их не записывайте.

Можно воспользоваться специальной программой — менеджером паролей, которая облегчит вам задачу, предложив сгенерированный надежный пароль, и будет этот пароль хранить.

Используйте двухфакторную авторизацию

Это способ защитить свой аккаунт от несанкционированного доступа, даже в том случае, если ваши логин и пароль знают злоумышленники. Обычно это выглядит так: первый рубеж — это логин и пароль, второй — специальный код, приходящий по SMS, в push-уведомлении или на электронную почту.

Не открывайте вложения подозрительных сообщений, а также не переходите по ссылкам в электронной почте, мессенджерах и соцсетях.

Это классический способ заражения компьютеров (или попытка перевести вас на фишинговую страницу). Никогда не открывайте вложение от неизвестного вам отправителя, а также не проходите по сомнительным ссылкам, чтобы не стать жертвой интернет-мошенников.

Не сообщайте персональную информацию незнакомым людям.

Мошенники могут маскироваться под знакомых ваших родителей, дальних родственников или сотрудников банка, писать вам в соцсетях или даже позвонить.

Свяжитесь напрямую с компанией, если вы получили подозрительный запрос.

Если звонящий просит вас предоставить какие-либо данные, положите трубку. Перезвоните в компанию напрямую по номеру телефона на ее официальном сайте и убедитесь, что вам звонили не мошенники.

Внимательно проверяйте адреса веб-сайтов, которые вы посещаете.

Обращайте внимание на URL-адреса сайтов, совпадают ли они с настоящими. Не переходите по ссылкам, которые отличаются от тех, что действительно принадлежат компаниям, даже на одну букву.

Когда устанавливаете приложения на смартфон, не давайте им доступ к тем функциям, которые им не нужны.

Например, условному приложению «Фонарик» явно ненужен доступ к вашим фотографиям и контактам.

Также давайте вспомним правила, которые касаются паролей.

Пароль — это одна из важнейших составляющих вашей приватности. Чтобы пароль был сложным для взлома, нужно придерживаться следующих правил:

Пароль должен быть надежным: иметь минимум 12 символов, а также содержать прописные и строчные буквы, цифры, специальные символы.

Меняйте пароль регулярно.

Если связка логин/пароль «утекла», то как можно скорее поменяйте пароль. Как это узнать? Есть специальные сайты для проверки утечек учетных записей. Обращайте внимание на новости о том, в каких сервисах произошли утечки.

В пароле не должно быть общедоступной или личной информации, например, имени вашего питомца или номера телефона.

Используйте разные уникальные пароли для разных сайтов.

Не храните пароли на листочках, в текстовых файлах на компьютере. Для этого лучше использовать специальные программы — менеджеры паролей.