**ПОМНИТЕ основные меры безопасности:**

***1. Не открывайте неизвестные вложения в письмах***

Если вы получили электронное письмо от подозрительного отправителя или получили от знакомого, но не договаривались об этом, или у вас есть подозрения относительно письма и его вложений в этом случае не открывайте вложенные файлы. документы, которые на первый взгляд выглядят вполне безобидно (например, документ word) могут содержать скрытые вредоносные программы. даже простая фотография может оказаться опасной.

***2. Не нажимайте, не подумав, на короткие ссылки***

***3. Осмотрительно используйте публичный wi-fi***, интернет наполнен информацией об опасности использования публичных wi-fi сетей, например в кафе, гостинице, аэропорту или в библиотеке. путем подмены hot spot или другими способами мошенники могут контролировать ваш трафик.

***4. Используйте разные пароли для различных аккаунтов***

Если кто-нибудь узнает или подберет ваш пароль, то он сможет подключиться к другим вашим аккаунтам. кроме того, любая атака на корпоративные базы данных (что также становится распространенным явлением) может осуществляться с вашими регистрационными данными.

***5. Обязательно установите и обновляйте антивирус***

Хорошая антивирусная программа – это лучший барьер, который вы можете установить между вашим компьютером и кибер-преступниками.

***6. Создавайте и обновляйте резервные копии документов: обращайте внимание на сообщения браузера о безопасности***

Когда вы перемещаетесь по сайтам, вы склонны действовать на автопилоте и часто игнорируете любые предупреждения, которые попадаются на глаза. если, например, chrome говорит, что сайт не безопасен, или firefox запрашивает подтверждение перед скачиванием файла, не стоит автоматически давать разрешение, даже не задумываясь – это наиболее простой путь к проникновению вредоносных программ на ваш компьютер.

***8. С осторожностью публикуйте в социальных сетях персональную информацию***

***9. Скачивайте только необходимые предложения и из известных источников***

Вредоносные программы, разработанные для мобильных устройств, распространяются все шире, и одна из главных опасностей – это скачивание приложений вне google play и apple store.

***10. С осторожностью подходите к любым финансовым сервисам, требующим ввода данных вашей карты, вашего счета, персональных данных, адресов, телефонов, особенно, если это связано с каким-то выигрышем, промо – акциями*** и .т.д

