**Что такое «кибер-гигиена», для чего она нужна?**

Кибергигиена - набор действий, выполняемых пользователями компьютеров и других устройств для повышения сетевой безопасности и обеспечения работоспособности системы.

Фактически это образ мышления и привычки с фокусом на безопасность, помогающие снизить количество нарушений в интернете и минимизировать вероятность поражения компьютера или электронного устройства.

1. Пользуйтесь легальными антивирусными программами, чтобы уменьшить вероятность заражения компьютера, а бесплатные продукты обычно имеют сильно урезанный функционал.

2. После приобретения и установки антивирусных программ регулярно их обновляйте. Без актуальных обновлений никакой «антивирус» не защитит эффективно компьютер.

Обеспечивайте регулярный запуск проверки системы (сканирование). Быструю проверку рекомендуется запускать раз в неделю, полную – раз в месяц.

3. Проверяйте подключаемые к компьютеру внешние носители информации (флеш-накопители, жесткие диски и т.д.), а так же файлы, скаченные из интернета.

4. Устанавливайте только знакомые программы, взятые из известных источников. Это поможет избежать проникновения вирусов, замаскированных под полезное программное обеспечение. Лучшие источники драйверов и программ – сайты непосредственных производителей.

5. Не используйте «пиратское» программное обеспечение. Использование взломанных программ чревато заражением компьютера, поскольку в генераторы ключей встраиваются троянские программы, клавиатурные шпионы и т.д.

6. Работая в интернете, обращайте внимание на то, на каком именно сайте вас просят ввести пароль, номер телефона или совершить какое-либо действие (бесплатно проверить компьютер на вирусы, скачать обновление и т.д.). Если вы не опытный пользователь и не уверенны в своих действиях – не предпринимайте этих действий. Злоумышленники часто пользуются неопытностью, подменяя адреса известных сайтов, предлагая скачать вирусы под видом обновлений программного обеспечение.

7. Используйте длинные и сложные пароли, сочетание цифр, строчных и заглавных букв. Это усложнит злоумышленникам доступ к вашей информации.

8. Делайте резервное копирование данных. С каждым днём всё больше распространяются вирусы‑вымогатели. Они блокируют устройство и угрожают удалить с него все данные, если вы не заплатите выкуп. Такие вирусы могут попасть на компьютер или смартфон, если вы перейдёте по ссылке в фишинговом письме или кликнете на фейковый рекламный баннер.

9. Не делитесь личной информацией в социальных сетях. Не публикуйте в открытом доступе дату своего рождения, не указывайте свой адрес, местоположение и контакты. Отключите геотеги на фотографиях. Хотя сами по себе такие данные кажутся безобидными, с их помощью преступники могут многое о вас узнать. Персональные данные пользователей собираются зачастую для последующего доступа к их финансам.

10. Регулярно проверяйте историю финансовых операций, включая выписки по картам, особенно кредитным. А раз в год запрашивайте свою кредитную историю, чтобы проверить, не открыты ли на ваше имя чужие займы.

При возможности настройте в банковском приложении двухфакторную аутентификацию (когда при входе нужно будет вводить не только пароль, но и код из СМС или пуш‑уведомления). Этот метод безопаснее, чем обычная активация приложения.