

Как соблюдать кибергигиену?

Эта памятка поможет защитить ваши персональные данные от киберпреступников и научит безопасному пользованию интернетом

Кибергигиена – это формирование полезных привычек, которые обеспечивают безопасную работу в интернете, чтобы не стать жертвой мошенников, а также уберечь от преступников конфиденциальные данные.

Храните пароли в безопасности

- Не используйте один и тот же пароль для нескольких приложений (социальные сети, мобильный банкинг и т.д.);
- Регулярно меняйте пароли;
- Используйте сложные пароли, в состав которых входят заглавные и строчные буквы, символы и цифры.

Не делитесь личными данными

- Не публикуйте в социальных сетях личную информацию – домашний адрес, геолокацию, личные фотографии, номер телефона, данные банковских карт;
- Проверьте настройки конфиденциальности в социальных сетях и убедитесь, что ваши личные данные не находятся в открытом доступе;
- Не участвуйте в онлайн-викторинах, играх и опросах, которые запрашивают вашу личную информацию;
- С осторожностью относитесь к разрешениям доступа для используемых приложений и сайтов. Им ни к чему знать ваше местонахождение или иметь доступ к камере;
- Совершайте все онлайн-транзакции на безопасных сайтах, веб-адреса которых начинаются с **https://**, а не с **http://**;
- Старайтесь не подключаться к публичным сетям Wi-Fi, когда пользуетесь мобильным банкингом. Например, уязвимость таких сетей в отелях и других местах отдыха часто привлекает кибермошенников.

Опасайтесь уловок социальной инженерии («атак на человека» используя психологические и социологические приёмы с целью разглашения вами конфиденциальной и личной информации).

- Не переходите по подозрительным ссылкам, по которым интуитивно нельзя определить необходимый источник (сайт), например: <http://qazwsx.qa.com.qz/qawssxvvb> и т.д. Пример неподозрительного: <https://1lombard.kz>

Не открывайте письма и вложения, выглядящие подозрительно и от незнакомых адресов;

- Не переходите по объявлениям, обещающим денежные призы и крупные скидки.

Установите антивирус

- Антивирус – надежный защитник ваших устройств и персональных данных. Используйте лицензионное и хорошо зарекомендовавшее себя антивирусное программное обеспечение, которое найдет и удалит вирусы и прочие вредоносные программы;

Обновляйте приложения и программное обеспечение

- Регулярно обновляйте приложения, браузеры, операционные системы и прошивки, чтобы использовать последние версии, в которых устранены возможные уязвимости безопасности;
- Удаляйте приложения, которыми не пользуетесь;
- Загружайте (скачивайте) приложения только из надежных официальных источников;
- Используйте лицензионные операционные системы и другие программы и приложения.

Используйте многофакторную аутентификацию

- Настройте защиту для всех основных учетных записей приложений (электронная почта, социальные сети, банковские приложения) с использованием многофакторной аутентификации – способа контроля доступа, при котором пользователю необходимо предъявить не менее двух реквизитов, подтверждающих его право на доступ (например, в дополнение к паролю ввести код из СМС). Общедоступными средствами многофакторной аутентификации являются Google Authenticator, Authy и др, инструкции по настройке которых размещены на официальных сайтах.

Делайте резервное копирование данных

- Проводите регулярное резервное копирование данных, храните копии на внешних носителях информации (жесткие диски SDD, HDD и т.д.);
- По возможности обеспечьте шифрование всех носителей информации, содержащих конфиденциальные данные, включая ноутбуки, планшеты, смартфоны, съемные диски. Шифрование может осуществляться самим устройством (ноутбуки, ПК, смартфоны) или с помощью специализированного программного обеспечения.
- Перед утилизацией или продажей ПК, планшета или смартфона, очистите память устройства, чтобы не дать доступ третьим лицам к вашим персональным данным.

Сохраняйте бдительность

- Не открывайте ссылки, которые вызывают у вас подозрение;
- Обращайте внимание на всплывающие окна и сообщения в вашем браузере, программах, операционной системе и на мобильном устройстве. Не нажимайте кнопки «ОК», «Одобрить» или «Принимаю», не ознакомившись с содержанием этих окон;
- Проявляйте особую осторожность при использовании финансовых и банковских приложений и сайтов – заходите только на официальные источники.