Бұл нұсқаулық жеке деректеріңізді киберқылмыскерлерден қорғауға көмектеседі және Интернетті қалай қауіпсіз пайдалану керектігін үйретеді.

Кибергигиена дегеніміз не?

Кибергигиена - *алаяқтардың құрбаны болмау үшін, сонымен қатар қылмыскерлерден құпия деректерді қорғау үшін Интернетте қауіпсіз жұмысты қамтамасыз ететін пайдалы әдеттерді қалыптастыру.*

Құпия сөздерді қауіпсіз сақтаңыз

- Бірнеше қосымшалар үшін бір құпия сөзді пайдаланбаңыз (әлеуметтік желілер, мобильді банкинг, т.б.).
- Құпия сөздерді жүйелі түрде өзгертіңіз.
- Бас және кіші әріптерді, таңбаларды және сандарды қамтитын күрделі құпия сөздерді пайдаланыңыз.

Жеке ақпаратты бөліспеңіз

- Әлеуметтік желілерде жеке ақпаратты – үй мекенжайын, геолокацияны, жеке фотосуреттерді, телефон нөмірін, банк картасының деректемелерін жариялауға болмайды.
- Әлеуметтік желілердегі құпиялылық параметрлерін тексеріңіз және жеке ақпаратыңыз жалпыға қолжетімді емес екеніне көз жеткізіңіз.
- Жеке ақпаратыңызды сұрайтын онлайн викториналарға, ойындарға немесе сауалнамаларға қатыспаңыз.
- Пайдаланатын қосымшалар мен сайттарға кіру рұқсаттары туралы абай болыңыз. Оларға сіздің орналасқан жеріңізді білудің немесе камераңызды пайдаланудың қажеті жоқ.
- Барлық онлайн транзакцияларды веб-мекенжайлары http:// емес, https:// деп басталатын қауіпсіз сайттарда жүргізіңіз.

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

Что такое кибергигиена?

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