Персональные данные и правила личной безопасности в сети Интернет

Уважаемые друзья, сегодня много говорится об опасностях, подстерегающих нас со всех сторон: это вред здоровью от распространения вируса; возможность психологического срыва в условиях тотальной самоизоляции; страх привыкнуть к жизни в виртуальном пространстве; угроза беспечного распространения персональных данных. Но разумный подход и соблюдение простых правил помогут избежать всех этих угроз.

Для сохранения здоровья мойте руки и пользуйтесь гигиеническими масками. Для интересного времяпрепровождения в самоизоляции займитесь саморазвитием, читайте книги. Во избежание погружения в виртуальную среду общайтесь со своими родными. А теперь о защите личных данных…

Ответим на несколько вопросов:

1) Какой объём персональных данных необходимо указывать социальных сетях?

2) Как скрыть данные личной страницы от посторонних?

3) Что дает установка пароля на мобильное устройство?

4) Куда ведут ссылки от неизвестных отправителей?

И так… Персональные данные – это личные сведения, принадлежащие исключительно Вам. Для регистрации в социальной сети или на образовательном ресурсе необязательно указывать настоящие фамилию и имя, достаточно ограничиться вымышленным именем – «никнеймом». Указание номера телефона, домашнего адреса или имен родителей будет лишним на странице, которую могут увидеть все пользователи сети Интернет.

В каждой социальной сети можно настроить доступ к Вашей странице. Вы выбираете тех, кто может видеть личную информацию: все пользователи, только друзья или друзья друзей. Используйте эту возможность.

На минутку задумаемся: что телефон знает о нас? Самый очевидный ответ: «Все!». Это и фотографии с отметками географических координат места, где они были созданы, контакты всех Ваших друзей и знакомых, Ваша переписка, заметки, календари, ящики электронной почты, отпечатки пальца, скан радужной оболочки глаза, порой даже реквизиты банковских карт. Попади гаджет в руки злоумышленника он получит исчерпывающие сведения о Вас. На случай, если устройство с Вашими персональными данными попадет в чужие руки и существуют пароли.

Безопасность устройства зависит также от настроек безопасности и наличия установленных антивирусных программ.

Не переходите по неизвестным ссылкам, которые получили от незнакомых отправителей, так как они могут вести на мошеннические ресурсы, содержащие вирусное программное обеспечение.

Не регистрируйтесь на сомнительных сайтах, требующих ввести Ваши персональные данные.

Впереди летние каникулы, время поездок и путешествий, но не теряйте бдительность, не указывайте в социальных сетях на всеобще обозрение даты

Исполнитель:
Тел.:

Вашего отсутствия дома и место, куда вы отправляетесь отдыхать. Не включайте функцию геолокации на Вашем устройстве без особой надобности.

Общайтесь на форумах, в социальных сетях с удовольствием. Если общение становится для Вас неприятным или вы чувствуете проявление в отношении Вас агрессии со стороны собеседников – не поддавайтесь на провокации, прекращайте общение.

В любой непонятной ситуации обращайтесь к родителям, старшим товарищам или в Управление Роскомнадзора по Амурской области по телефону (4162) 494028.

Берегите свое здоровье и персональные данные!