

В современном мире цифровые технологии пронизывают все сферы жизни. Для пенсионеров и людей старшего возраста развитие навыков цифровой грамотности особенно важно, так как это помогает им получать доступ к важной информации, безопасно пользоваться онлайн-сервисами и при этом избегать встреч с мошенниками. Чем лучше человек понимает, как устроена цифровая среда, тем меньше шансов, что он станет жертвой обмана.

Кроме того, освоение цифровых технологий помогает пожилым людям сохранять социальные связи и активный образ жизни. Они могут общаться с родственниками и друзьями онлайн, записываться к врачу, заказывать товары и даже осваивать новые хобби.

ОСНОВНЫЕ ОПАСНОСТИ ИНТЕРНЕТА

- Кража персональных данных.
- Утечки данных.
- Вредоносные программы и вирусы.
- Фишинговые и мошеннические электронные письма.
- Поддельные сайты.
- Интернет-мошенничество.
- Мошенничество на сайтах и в приложениях для знакомств.
- Неприемлемый контент.
- Кибербуллинг.
- Неверные настройки конфиденциальности.



Меры предосторожности при работе в интернете

ПРАВИЛА ЦИФРОВОЙ ГРАМОТНОСТИ ПРОСТЫ:

1 Проверяйте подлинность сайта, на котором вас просят ввести свои данные или данные карт. Чаще всего мошенники подделывают сайты: «Госуслуги» и другие государственные порталы, сайты банков, страницы оплаты в интернет-магазинах. **ПОМНИМ**, что на незнакомых или сомнительных сайтах нельзя вводить свои персональные данные или данные своих банковских карт. Порталы и сайты, которыми часто пользуетесь, лучше поместить во вкладку «избранное».

2 При поиске информации в интернете проверяйте информацию, которую находите. Не доверяйте фейкам. Фейк – это целенаправленно распространяемая ложная информация в интернете, которую специально создают, чтобы запутать, ввести в заблуждение или посеять панику среди граждан.

ПОМНИМ, чтобы не попасться на провокацию, важно искать оригинальный источник новости, откуда она начала распространяться, а также доверять только качественной прессе.

3 Никогда не предоставляйте ваши персональные данные незнакомым людям. Персональные данные — это информация о человеке, по которой его можно идентифицировать. Поэтому предоставить свои персональные данные — это все равно, что пустить незнакомца к себе домой или отдать ему ключи от квартиры. Зная ваши персональные данные мошенники, могут взять на вас кредит или украсть данные карт и накопительных счетов. **ПОМНИМ**, персональные данные в сети помогают сформировать цифровой двойник человека, их нужно охранять.

4 Игнорируйте спам и сообщения во всплывающих окнах. Спам – это нежелательные сообщения в любой форме, которые отправляются в большом количестве. Чаще всего спам отправляется в форме коммерческих электронных писем, присланных на большое количество адресов, а также через мгновенные и текстовые сообщения (SMS), социальные медиа или даже голосовую почту. Через такую массовую рассылку приходят не только безобидные рекламные предложения, но и ссылки на вредоносные программы или фишинговые сайты. **ПОМНИМ**, не

стоит открывать письма от незнакомых адресантов. Внимательно стоит относиться к любым присланным ссылкам – даже если это сообщения от хорошо знакомых вам людей. Их почтой или аккаунтом могли воспользоваться мошенники. Если сомневаетесь, перезвоните отправителю и уточните детали.

Соблюдайте меры осторожности при общении в социальных сетях. Социальные сети – это интернет-площадки для общения, обмена информацией и контентом, прочих социальных взаимодействий. Например, «Одноклассники», «ВКонтакте». В социальных сетях не рекомендуется публиковать фотографии, которые потом можно было бы использовать против вас, распространять личные данные. Внимательно относитесь к виртуальным собеседникам, которых вы не знаете лично. Человек может представиться чужим именем, изменить личную информацию о себе, чтобы втереться в доверие или использовать в корыстных целях информацию о вас. Если вы считаете, что общающийся с вами человек вызывает подозрения и ведет себя необычно, лучше прекратите общение с ним. **ПОМНИМ**, что, если сделать свои аккаунты в соцсетях закрытыми – это затруднит мошенникам доступ к вашим данным.

Записывайте на бумажных носителях ваши пароли и PIN-коды. Не храните их в компьютере. Пароль – это секретная комбинация цифр, букв и других знаков для получения доступа к различным данным или компьютерной программе. Не используйте в пароле свои имя, фамилию, клички животных, информацию о родственниках. Создавайте пароль из не менее чем 8-10 символов и добавляйте в него строчные и заглавные буквы, цифры и символы. Меняйте пароль хотя бы 1 раз в месяц. **ПОМНИМ**, что пароли и PIN-коды не должны дублироваться в разных сервисах.

Пользуйтесь антивирусом. Антивирус – это программное обеспечение, состоящее из нескольких слоев защиты и предназначенное для обнаружения, блокировки и удаления вирусов, вредоносных программ, а также для защиты пользователя от других киберугроз. **ПОМНИМ**, что актуальное антивирусное программное обеспечение поможет защитить вашу конфиденциальную информацию от мошенников.