Памятка «Правила безопасного интернета при организации дистанционного обучения»

Ресурс

Угроза 1

Утечка персональных данных

Персональные данные (имя, дата рождения, паспортные и контактные данные, медицинская и финансовая информация, данные о местоположении) очень ценны для мошенников. Их утечка в интернете может привести к мошенничеству - с их помощью преступники входят в доверие к жертве и отнимают деньги.

1. Ограничьте доступ к личным данным в соцсетях

Настройте приватность так, чтобы только хорошо знакомые люди видели вашу информацию, местоположение, список друзей и т.д.

2. Не публикуйте конфиденциальные данные

Не размещайте в сети Интернет фотографии документов, банковских карт, адресов, номеров телефонов.

3. Будьте осторожны с друзьями в соцсетях

Добавляйте в друзья только знакомых людей, проверяйте подлинность аккаунтов.

4. Используйте разные email-адреса

Для личной переписки, регистрации в интернет-магазинах и рабочих задач лучше применять отдельные почтовые ящики.

5. Контролируйте разрешения приложений на смартфоне

Не давайте доступ к камере, микрофону, геолокации и контактам приложениям, которые в этом не нуждаются.

6. Создайте и используйте безопасные пароли

- Длинный: не менее 12–15 символов.
- Сложный: комбинация строчных и прописных букв, цифр и специальных символов.
- Уникальный: для каждого аккаунта создавайте отдельный пароль.
- Без личных данных: не включайте в пароль имя, дату рождения, кличку питомца и т.п.

Памятка «Правила безопасного интернета при организации дистанционного обучения»

Ресурс

Угроза 2

Вредоносные/мошеннические ссылки (фишинг)

Фишинг (от англ. fishing — «рыбная ловля») - это интернет мошенничество: злоумышленники пытаются выманить личные данные - пароли, логины, реквизиты карт и т.д. Для этого они создают поддельные сайты и рассылают фальшивые письма или сообщения - например, от имени сервисов, коллег или администрации.

1. Проверяйте адрес отправителя

Злоумышленники часто используют адреса, похожие на официальные (например, gosus1ugi вместо gosuslugi).

2. Не переходите по ссылкам

Если письмо сообщает о проблеме с аккаунтом, зайдите на сайт сервиса напрямую через браузер, а не через ссылку в письме.

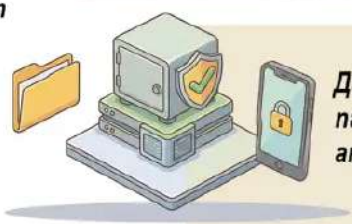
3. Не вводите личные данные

Логины, пароли, данные карт на незнакомых сайтах.

4. Изучайте URL сайта

Перед вводом номера телефона, пароля или данных карты проверьте адресную строку. Ищите опечатки и наличие замочка (HTTPS).

5. Используйте двухфакторную аутентификацию



Даже если мошенники узнают пароль, они не смогут войти в аккаунт без проверочного кода.

6. Настройте антифишинг

Включите встроенные фильтры безопасности в браузере и почтовом сервисе.

7. Не поддавайтесь на эмоции

Фишинг часто строится на запугивании («Ваш счет заблокирован») или заманчивых предложениях («Вы выиграли»).

Памятка «Правила безопасного интернета при организации дистанционного обучения»

Ресурс

Угроза 3

Вредоносное программное обеспечение и вирусы

Программы, предназначенные для повреждения данных и несанкционированного доступа к системам, могут блокировать информацию, похищать личные данные или использовать устройство для атак. Установка неизвестных программ из интернета даёт злоумышленникам возможность управлять вашим устройством, записывать разговоры и включать камеру.

1. Используйте антивирусные программы

Регулярно обновляйте антивирусное ПО для защиты от новых угроз.

2. Обновляйте программное обеспечение

Установите последние обновления для операционной системы и приложений для устранения уязвимостей. Не игнорируйте уведомления об обновлении - в них закрываются «дыры», через которые могут проникнуть вирусы.

3. Будьте осторожны с вложениями

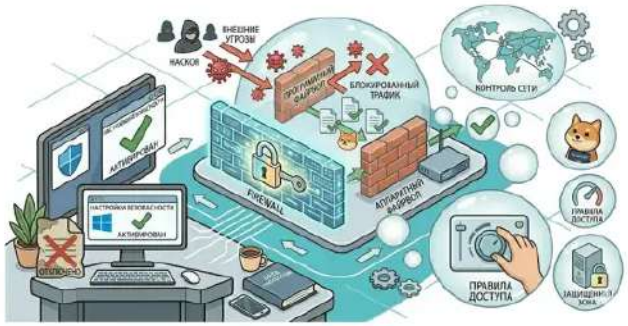
БУДЬТЕ ОСТОРОЖНЫ

Не открывайте файлы (особенно .exe, .zip, .scr) из подозрительных писем - в них может быть вирус.

4. Регулярно создавайте резервные копии

Храните копии важных файлов на внешних носителях либо в облаке - так вы не потеряете данные, если вирус удалит их с ПК.

5. Используйте файрвол



Включите файрвол для защиты от несанкционированного доступа.