6 ГЛАВА Правила безопасности при работе в мобильных приложениях видеообщения

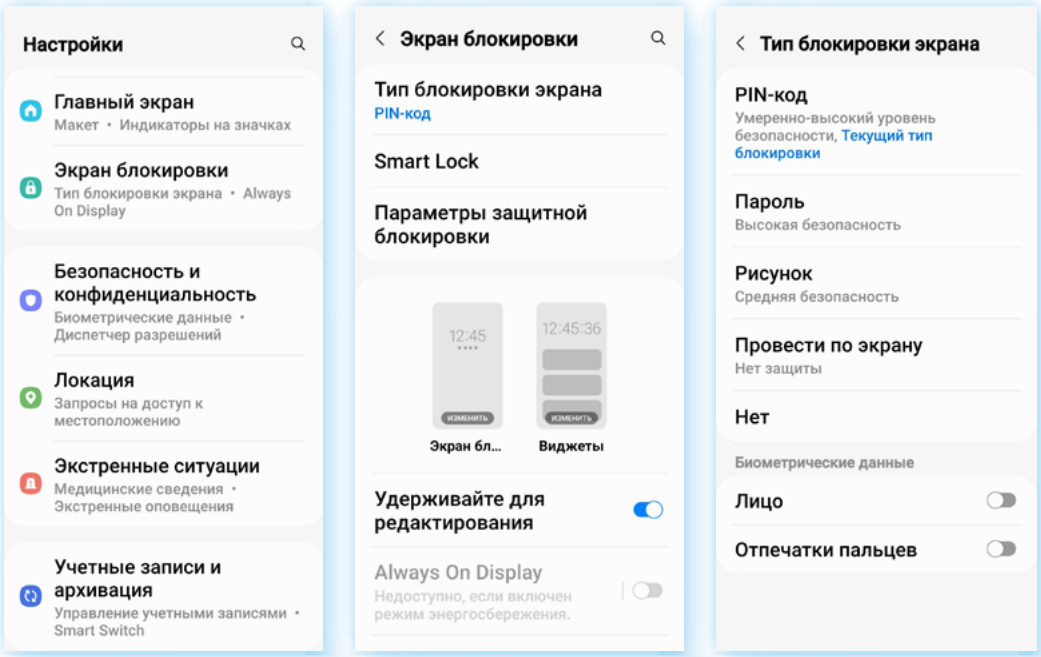
Правила безопасности при работе в программах для видеообщения в интернете

Поскольку все программы для видеообщения работают через сеть интернет, то при работе с ними нужно соблюдать общие правила безопасности при работе в интернете. Но также стоит обратить особое внимание на некоторые из них.

Для установки скачивайте программы для видеообщения с официального сайта разработчика или из магазина приложений. Перед тем как скачать программу, читайте ее описание и отзывы о ней.

Если программа установлена на вашем мобильном телефоне или планшете, старайтесь не оставлять мобильные устройства без присмотра. Рекомендуется поставить блокировку экрана на смартфон и на планшетный компьютер. Это можно сделать в **«Личных данных»**, в разделе **«Настройки»**. Современные смартфоны, например, предлагают блокировку экрана телефона по отпечатку пальца 6.1.

6.1



Также после установки изучите настройки профиля в программе. Там обязательно должен быть раздел, где вы сможете настроить приватность, безопасность и конфиденциальность вашей работы в программе.

Ограничьте доступ к вашей личной информации, выберите настройки, которые помогут вам сэкономить интернет-трафик (объем передачи данных через интернет).

В групповых и личных чатах не указывайте личные данные, например, ПИН-код от банковской карты или пароли от личных страничек в социальных сетях или на других сайтах.

Если вы планируете собирать благотворительную помощь, для этих целей следует оформить отдельную банковскую карту и на страничке сообщать только ее номер и банк, где она открыта. Этого достаточно, чтобы пользователи могли оказать помощь.

Обязательно установите на свое компьютерное устройство антивирус.

Никогда не переходите по ссылкам в сообщениях, если они получены от незнакомых пользователей, а увидев подозрительные ссылки от своих собеседников, уточните, что в них.

Иногда после перехода по ссылке можно получить в свое компьютерное устройство вирус, считывающий ваши личные данные.

Мошенники часто используют мессенджеры для обмана пользователей. Их главная задача — получить ваши личные данные или ваши денежные средства. Это могут быть сообщения с незнакомых номеров с предложениями заработка, сообщения от банков о блокировке счета или пугающие сообщения, касающиеся ваших близких.

Сообщения о предложении заработка можно просто удалить. В остальных случаях — перезвоните своим близким, убедитесь, что с ними все в порядке, перезвоните в банк или зайдите в приложение онлайн-банка и проверьте состояние своего счета. Здесь же, в приложении банка, вы можете найти пункт **«Сообщить о мошенниках»** в разделе **«Безопасность»**. Сообщите номер телефона, с которого поступил звонок или сообщение.

Часто мошенники звонят через мессенджеры и представляются сотрудниками банков, полицейскими, адвокатами и просят сообщить данные банковской карты или перевести деньги на некий счет. Что делать:

- если вы видите звонок через мессенджер от незнакомого пользователя, можно не брать трубку. Если вы уверены, что звонил мошенник, заблокируйте контакт;
- относитесь внимательно к новым знакомым. Если у вас выспрашивают слишком много личной информации, касающейся наличия финансов, адреса, лучше прекратите общение;
- публичные группы, каналы в некоторых программах позволяют делать покупки онлайн. Прежде чем заплатить деньги, внимательно изучите страничку магазина или продавца, почитайте о них отзывы в интернете, задайте дополнительные вопросы;
- для оплаты в интернете заведите отдельную банковскую карту, на которую переводите ровно столько средств, сколько нужно для покупки.

Подробно о правилах безопасности при финансовых расчетах в сети — в главе 1 модуля 4 «Оплата товаров и услуг через интернет: полезные сервисы и платежные устройства» расширенного курса программы «Азбука интернета».

Относитесь к этим правилам как к любым другим в реальной жизни: не переходить дорогу на красный свет, не оставлять кошелек на скамейке и т.д.

Интернет — огромное виртуальное пространство, в котором также нужно соблюдать осторожность.

Контрольные вопросы

1. Какие меры предосторожности нужно соблюдать, работая в программах для видеообщения?
2. Как вы поступите, если вам пришло сообщение от незнакомого человека с предложением перейти по ссылке?
3. На какие разделы программ и приложений для видеообщения стоит обратить особое внимание в целях собственной безопасности?
4. Какие правила безопасности нужно соблюдать при проведении финансовых расчетов в сети интернет?