Приложение 2

ПАМЯТКА

- Блокируйте свой телефон и используйте хороший пароль;
- Не говорите пароль никому;
- Обновляйте операционную систему устройства и установленные приложения;
- Настройте автоматические обновления: многие программы автоматически подключаются и обновляются. Это позволяет защитить систему от новых угроз;
- Выключайте Wi-Fi, bluetooth, геолокацию – когда ими не пользуетесь;
- Хорошо подумайте, перед тем как ставить новое незнакомое приложение, скачивать музыку и фильмы;
- Остерегайтесь отправлять свою личную или конфиденциальную информацию;
- Не нажимайте на ссылки и не открывайте файлы от незнакомых людей (или даже от знакомых, если вы не ждете этого – позвоните и спросите отправлял ли Вам коллега письмо);
- Аккуратно общайтесь с незнакомцами онлайн;
- Если есть сомнения, не подключайтесь: ссылки в электронной почте, заметки в социальных сетях, сообщения и Интернет-реклама зачастую создаются киберпреступниками;
- Если письмо выглядит подозрительно, даже если вы знаете адресата, лучше удалите письмо, если это уместно, отметьте, как нежелательную почту/спам;
- Следите за защищённостью учетных записей: многие ресурсы предлагают дополнительные способы идентификации, чтобы удостовериться кто вы (например, привяжите учетную запись к телефону и используйте двухфакторный вход – пароль+SMS пароль); Это нужно включить в социальной сети, почте и облачном хранилище данных (например, iCloud);
- Создавайте длинные и сложные пароли: комбинации букв с цифрами и символами создают более безопасный пароль;
- Новая учетная запись, уникальный пароль: во вновь создаваемом пароле комбинируйте буквы, цифры, верхний и нижний регистр. Можно использовать стихотворения и строчки песен для паролей – пишите на английском, смотрите на русские буквы;
- Знайте об основных способах кражи информации и угрозах информационной безопасности. Идти в ногу со временем – лучший способ оставаться в безопасности в Интернете;
- Спрашивайте разрешения своих друзей и коллег, чтобы поделиться их фотографиями и любой другой информацией о них;

- Знайте, что любой текст, который вы отправите, может стать доступен всем – подумайте об этом дважды;
- Все, что вы загружаете в Интернет, включая видео и фото – может стать доступно всем и остаться в Интернете навсегда;
- Подумайте, прежде чем действовать: опасайтесь сообщений, которые призывают Вас действовать немедленно, предлагают что-то, что звучит слишком хорошо, чтобы быть правдой, или просят предоставить личную информацию;
- Делайте резервные копии каждую неделю: электронная копия должна содержать файлы, почту, музыку, фото и другую цифровую информацию. Сделайте резервную копию и храните ее в безопасном месте (не на своем компьютере). Это касается как компьютера, так и мобильного телефона.