Держите устройства «в чистоте».

- **Необходимо регулярно обновлять системы защиты**. Убедитесь, что все мобильные устройства в вашем доме снабжены новейшими системами защиты информации. Для этого может потребоваться синхронизация устройств с компьютером.
- **Настройте автоматические обновления**: Многие программы автоматически подключаются и обновляются. Это позволяет защитить систему от новых угроз.
- **Защитите все устройства, подключенные к Интернету**: компьютеры, смартфоны, игровые приставки и другие устройства с доступом в Интернет нуждаются в защите от вирусов и вредоносных программ.
- **«Подключил и проверил»:** USB и другие внешние устройства могут быть заражены вирусами и вредоносным ПО. Сканируйте такие устройства на предмет вредоносов, как только подключаете их.

Защитите свою личную информацию.

- **Следите за защищённостью учетных записей**: Многие ресурсы предлагают дополнительные способы идентификации, чтобы удостоверится, кто вы;
- **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;
- **Запишите пароль и держите его в безопасном месте**: Каждый может забыть пароль. Держите список паролей в надежном месте вдали от компьютера.
- **Ваше присутствие в Интернете**: Установите режим конфиденциальности и безопасности для веб-сайтов. Всем не обязательно знать, с кем и когда вы обмениваетесь информацией.

Безопасность коммникаций.

- **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.
- **Получите сведенья о точках доступа Wi-Fi**: отрегулируйте настройки безопасности на ваших устройствах, чтобы ограничить доступ к ним.
- **Защитите свои деньги**: при совершении банковских операций и покупок в интернете, пользуйтесь адресами, начинающимися на "https:// ". Это означают, что сайт

принимает дополнительные меры для обеспечения безопасности своих клиентов. "http :/ /" не является безопасным.

Будьте в курсе.

- **Идти в ногу со временем – лучший способ оставаться в безопасности в Интернете.** Регулярно читайте информацию о безопасности в Сети, поделитесь ей с друзьями, семьей и коллегами, с призывом их быть подкованными в этом вопросе.
- **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:** электронная копия должна содержать ваш музыку, фото и другую цифровую информацию. Сделайте резервную копию и храните ее в безопасном месте.

Будьте добропорядочным пользователем Сети.

- **Безопасное для меня - недоступное для всех**: распространяйте принципы безопасной работы на свой круг общения - дом, коллеги на работе, весь мир. Как показывает практика, мы – глобальное цифровое сообщество.
- **Другие могут передавать информацию о вас точно так же, как и вы о них**
- **Помогайте обществу бороться с киберпреступностью:** сообщайте о киберпреступлениях или украденных через Интернет деньгах на www.group-ib.ru.

Посетите http://www.stopthinkconnect.org, чтобы получить дополнительные сведения.