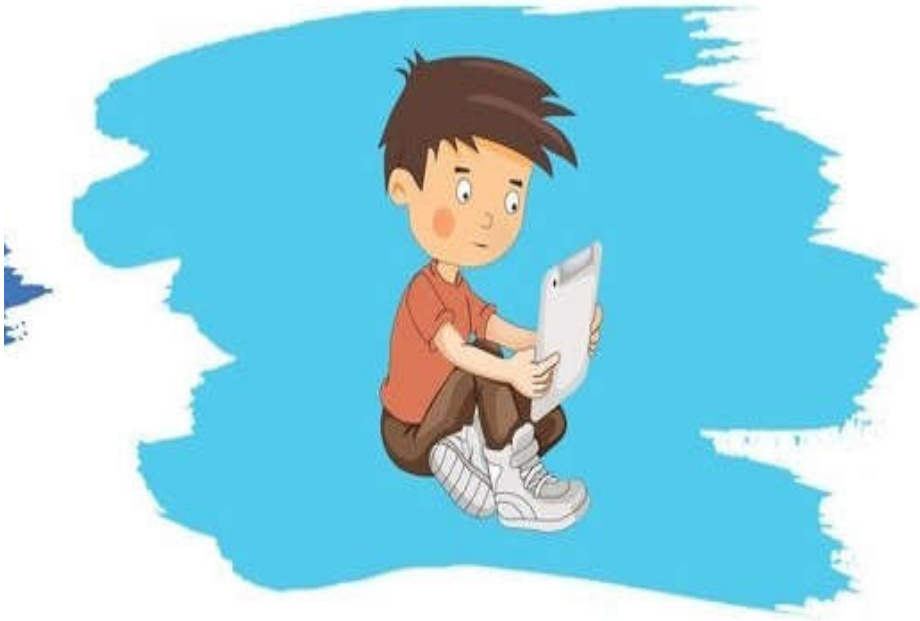
ИНФОРМАЦИОННАЯ ПАМЯТКА
ПО ВОПРОСАМ КИБЕРБЕЗОПАСНОСТИ

СОЦИАЛЬНЫЕ СЕТИ

- ОГРАНИЧЬТЕ СПИСОК ДРУЗЕЙ. У ВАС В ДРУЗЬЯХ НЕ ДОЛЖНО БЫТЬ СЛУЧАЙНЫХ И НЕЗНАКОМЫХ ЛЮДЕЙ;
- ЗАЩИЩАЙТЕ СВОЮ ЧАСТНУЮ ЖИЗНЬ. НЕ УКАЗЫВАЙТЕ ЛИЧНУЮ ИНФОРМАЦИЮ;
- ЗАЩИЩАЙТЕ СВОЮ РЕПУТАЦИЮ. ПОДУМАЙТЕ, ПРЕЖДЕ ЧЕМ ЧТО-ТО ОПУБЛИКОВАТЬ ИЛИ ЗАГРУЗИТЬ;
- ЕСЛИ ВЫ ГОВОРИТЕ С ЛЮДЬМИ, КОТОРЫХ НЕ ЗНАЕТЕ, НЕ ИСПОЛЬЗУЙТЕ СВОЮ ЛИЧНУЮ ИНФОРМАЦИЮ;
- ИЗБЕГАЙТЕ РАЗМЕЩЕНИЯ ФОТОГРАФИЙ В ИНТЕРНЕТЕ, ГДЕ ВЫ ИЗОБРАЖЕНЫ НА МЕСТНОСТИ, ПО КОТОРОЙ МОЖНО ОПРЕДЕЛИТЬ ВАШЕ МЕСТОПОЛОЖЕНИЕ;
- ПРИ РЕГИСТРАЦИИ В СОЦИАЛЬНОЙ СЕТИ НЕОБХОДИМО ИСПОЛЬЗОВАТЬ СЛОЖНЫЕ ПАРОЛИ;
- ДЛЯ СОЦИАЛЬНОЙ СЕТИ, ПОЧТЫ И ДРУГИХ САЙТОВ НЕОБХОДИМО ИСПОЛЬЗОВАТЬ РАЗНЫЕ ПАРОЛИ.



МОБИЛЬНЫЙ ТЕЛЕФОН

- БУДЬТЕ ОСТОРОЖНЫ, ВЕДЬ КОГДА ВАМ ПРЕДЛАГАЮТ БЕСПЛАТНЫЙ КОНТЕНТ;
- НЕОБХОДИМО СВОЕВРЕМЕННО ОБНОВЛЯТЬ ОПЕРАЦИОННУЮ СИСТЕМУ ВАШЕГО СМАРТФОНА;
- ИСПОЛЬЗУЙТЕ АНТИВИРУСНЫЕ ПРОГРАММЫ ДЛЯ МОБИЛЬНЫХ ТЕЛЕФОНОВ;
- НЕ ЗАГРУЖАЙТЕ ПРИЛОЖЕНИЯ ОТ НЕИЗВЕСТНОГО ИСТОЧНИКА, ОНИ МОГУТ СОДЕРЖАТЬ ВИРУСЫ;
- ПОСЛЕ ВЫХОДА С САЙТА, ГДЕ ВВОДИЛИ ЛИЧНУЮ ИНФОРМАЦИЮ, УДАЛИТЕ COOKIES;
- ПРОВЕРЯЙТЕ, КАКИЕ ПЛАТНЫЕ УСЛУГИ АКТИВИРОВАНЫ НА ВАШЕМ НОМЕРЕ ТЕЛЕФОНА;
- ДАВАЙТЕ СВОЙ НОМЕР МОБИЛЬНОГО ТЕЛЕФОНА ТОЛЬКО ЛЮДЯМ, КОТОРЫМ ДОВЕРЯЕТЕ;
- BLUETOOTH ДОЛЖЕН БЫТЬ ВЫКЛЮЧЕН, КОГДА ВЫ ИМ НЕ ПОЛЬЗУЕТЕСЬ.

КОМПЬЮТЕРНЫЕ ВИРУСЫ

- ИСПОЛЬЗУЙТЕ СОВРЕМЕННЫЕ ОПЕРАЦИОННЫЕ СИСТЕМЫ;
- ПОСТОЯННО УСТАНАВЛИВАЙТЕ ПАТЧИ И ДРУГИЕ ОБНОВЛЕНИЯ СВОЕЙ ОПЕРАЦИОННОЙ СИСТЕМЫ. СКАЧИВАЙТЕ ИХ ТОЛЬКО С ОФИЦИАЛЬНОГО САЙТА РАЗРАБОТЧИКА ОС;
- РАБОТАЙТЕ НА СВОЕМ КОМПЬЮТЕРЕ ПОД ПРАВАМИ ПОЛЬЗОВАТЕЛЯ, А НЕ АДМИНИСТРАТОРА;
- ИСПОЛЬЗУЙТЕ АНТИВИРУСНЫЕ ПРОГРАММНЫЕ ПРОДУКТЫ ИЗВЕСТНЫХ ПРОИЗВОДИТЕЛЕЙ;
- ОГРАНИЧЬТЕ ФИЗИЧЕСКИЙ ДОСТУП К КОМПЬЮТЕРУ ДЛЯ ПОСТОРОННИХ ЛИЦ;
- ИСПОЛЬЗУЙТЕ ВНЕШНИЕ НОСИТЕЛИ ИНФОРМАЦИИ ТОЛЬКО ИЗ ПРОВЕРЕННЫХ ИСТОЧНИКОВ;
- НЕ ОТКРЫВАЙТЕ КОМПЬЮТЕРНЫЕ ФАЙЛЫ, ПОЛУЧЕННЫЕ ИЗ НЕНАДЁЖНЫХ ИСТОЧНИКОВ.

ЭЛЕКТРОНАЯ ПОЧТА

- ВЫБИРАЙТЕ ИЗВЕСТНЫЕ ПОЧТОВЫЕ СЕРВИСЫ;
- НЕ УКАЗЫВАЙТЕ В ЛИЧНОЙ ПОЧТЕ ЛИЧНУЮ ИНФОРМАЦИЮ;
- ВЫБЕРИТЕ СЛОЖНЫЙ ПАРОЛЬ И ИСПОЛЬЗУЙТЕ ДВУХЭТАПНУЮ АВТОРИЗАЦИЮ;
- ЕСЛИ ЕСТЬ ВОЗМОЖНОСТЬ НАПИСАТЬ САМОМУ СВОЙ ЛИЧНЫЙ ВОПРОС, ИСПОЛЬЗУЙТЕ ЭТУ ВОЗМОЖНОСТЬ;
- ИСПОЛЬЗУЙТЕ НЕСКОЛЬКО ПОЧТОВЫХ ЯЩИКОВ. ПЕРВЫЙ ДЛЯ ЧАСТНОЙ ПЕРЕПИСКИ С АДРЕСАТАМИ, КОТОРЫМ ВЫ ДОВЕРЯЕТЕ. И НЕ ИСПОЛЬЗУЙТЕ ЕГО ПРИ РЕГИСТРАЦИИ НА ФОРУМАХ И САЙТАХ;
- НЕ ОТКРЫВАЙТЕ ФАЙЛЫ И ДРУГИЕ ВЛОЖЕНИЯ В ПИСЬМАХ ДАЖЕ ЕСЛИ ОНИ ПРИШЛИ ОТ ВАШИХ ДРУЗЕЙ;
- ПОСЛЕ ОКОНЧАНИЯ РАБОТЫ НА ПОЧТОВОМ СЕРВИСЕ НЕ ЗАБУДЬТЕ НАЖАТЬ НА «ВЫЙТИ».

WI-FI СЕТИ

- НЕ ПЕРЕДАВАЙТЕ СВОЮ ЛИЧНУЮ ИНФОРМАЦИЮ ЧЕРЕЗ ОБЩЕДОСТУПНЫЕ WI-FI СЕТИ;
- ИСПОЛЬЗУЙТЕ И ОБНОВЛЯЙТЕ АНТИВИРУСНЫЕ ПРОГРАММЫ И БРАНДМАУЭР;
- ПРИ ИСПОЛЬЗОВАНИИ WI-FI ОТКЛЮЧИТЕ ФУНКЦИЮ «ОБЩИЙ ДОСТУП К ФАЙЛАМ И ПРИНТЕРАМ»;
- НЕ ИСПОЛЬЗУЙТЕ ПУБЛИЧНЫЙ WI-FI ДЛЯ ПЕРЕДАЧИ ЛИЧНЫХ ДАННЫХ, НАПРИМЕР, ДЛЯ ВЫХОДА В СОЦИАЛЬНЫЕ СЕТИ ИЛИ В ЭЛЕКТРОННУЮ ПОЧТУ;
- ИСПОЛЬЗУЙТЕ ТОЛЬКО ЗАЩИЩЕННОЕ СОЕДИНЕНИЕ ЧЕРЕЗ HTTPS А НЕ HTTP, Т.Е. ПРИ НАБОРЕ ВЕБ-АДРЕСА ВВОДИТЕ ИМЕННО «HTTPS://»;
- В МОБИЛЬНОМ ТЕЛЕФОНЕ ОТКЛЮЧИТЕ ФУНКЦИЮ «ПОДКЛЮЧЕНИЕ К WI-FI АВТОМАТИЧЕСКИ».
- НЕ ДОПУСКАЙ АВТОМАТИЧЕСКОГО ПОДКЛЮЧЕНИЯ УСТРОЙСТВА К WI-FI БЕЗ ВАШЕГО СОГЛАСИЯ.

КИБЕРБУЛИНГ

- НЕ БРОСАЙТЕСЬ В БОЙ. ЕСЛИ ВЫ НАЧНЕТЕ ОТВЕЧАТЬ ОСКОРБЛЕНИЯМИ НА ОСКОРБЛЕНИЯ, ТОЛЬКО БОЛЬШЕ РАЗОЖЖЕТЕ КОНФЛИКТ;
- УПРАВЛЯЙТЕ СВОЕЙ КИБЕРРЕПУТАЦИЕЙ;
- АНОНИМНОСТЬ В СЕТИ МНИМАЯ. НЕ СТОИТ ВЕСТИ ХУЛИГАНСКИЙ ОБРАЗ ВИРТУАЛЬНОЙ ЖИЗНИ;
- ВЕДИТЕ СЕБЯ ВЕЖЛИВО;
- ИГНОРИРУЙТЕ ЕДИНИЧНЫЙ НЕГАТИВ. ОБЫЧНО АГРЕССИЯ ПРЕКРАЩАЕТСЯ НА НАЧАЛЬНОЙ СТАДИИ;
- ОГРАНИЧЬТЕ ДОСТУП АГРЕССОРУ. ЗАБЛОКИРУЙТЕ ОТПРАВКУ СООБЩЕНИЙ ДЛЯ ЭТОГО АДРЕСАТА;
- ЕСЛИ ВЫ СВИДЕТЕЛЬ КИБЕРБУЛЛИНГА. ВАШИ ДЕЙСТВИЯ: ВЫСТУПИТЬ ПРОТИВ ПРЕСЛЕДОВАТЕЛЯ, ПОКАЗАТЬ ЕМУ, ЧТО ЕГО ДЕЙСТВИЯ ОЦЕНИВАЮТСЯ НЕГАТИВНО, ПОДДЕРЖАТЬ ЖЕРТВУ.

ЭЛЕКТРОННЫЕ ДЕНЬГИ

- ПРИВЯЖИТЕ К СЧЕТУ МОБИЛЬНЫЙ ТЕЛЕФОН. ЭТО САМЫЙ УДОБНЫЙ И БЫСТРЫЙ СПОСОБ ВОССТАНОВИТЬ ДОСТУП К СЧЕТУ. ПРИВЯЗАННЫЙ ТЕЛЕФОН ПОМОЖЕТ, ЕСЛИ ЗАБУДЕТЕ СВОЙ ПЛАТЕЖНЫЙ ПАРОЛЬ ИЛИ ЗАЙДЕТЕ НА САЙТ С НЕЗНАКОМОГО УСТРОЙСТВА;
- ИСПОЛЬЗУЙТЕ ОДНОРАЗОВЫЕ ПАРОЛИ. ПОСЛЕ ПЕРЕХОДА НА УСИЛЕННУЮ АВТОРИЗАЦИЮ ВАМ УЖЕ НЕ БУДЕТ УГРОЖАТЬ ОПАСНОСТЬ КРАЖИ ИЛИ ПЕРЕХВАТА ПЛАТЕЖНОГО ПАРОЛЯ;
- ВЫБЕРИТЕ СЛОЖНЫЙ ПАРОЛЬ.НАДЕЖНЫЕ ПАРОЛИ – ЭТО ПАРОЛИ, КОТОРЫЕ СОДЕРЖАТ НЕ МЕНЕЕ 8 ЗНАКОВ И ВКЛЮЧАЮТ В СЕБЯ СТРОЧНЫЕ И ПРОПИСНЫЕ БУКВЫ, ЦИФРЫ И НЕСКОЛЬКО СИМВОЛОВ,
- ТАКИЕ КАК ЗНАК ДОЛЛАРА, ФУНТА, ВОСКЛИЦАТЕЛЬНЫЙ ЗНАК И Т.П. НАПРИМЕР, STRONG!;
- НЕ ВВОДИТЕ СВОИ ЛИЧНЫЕ ДАННЫЕ НА САЙТАХ, КОТОРЫМ НЕ ДОВЕРЯЕТЕ.

ФИШИНГ

- ЕСЛИ ВЫ ПОДОЗРЕВАЕТЕ, ЧТО ВАША АНКЕТА БЫЛА ВЗЛОМАНА, НЕОБХОДИМО ЗАБЛОКИРОВАТЬ ЕЕ И СООБЩИТЬ АДМИНИСТРАТОРАМ РЕСУРСА;
- ИСПОЛЬЗУЙТЕ БЕЗОПАСНЫЕ ВЕБ-САЙТЫ, ИНТЕРНЕТ-МАГАЗИНЫ И ПОИСКОВЫЕ СИСТЕМЫ;
- ИСПОЛЬЗУЙТЕ СЛОЖНЫЕ И РАЗНЫЕ ПАРОЛИ. ЕСЛИ ЗЛОУМЫШЛЕННИКИ ВЗЛОМАЮТ ВАШ АККАУНТ, ТО ПОЛУЧАТ ДОСТУП ТОЛЬКО К ОДНОМУ ВАШЕМУ ПРОФИЛЮ В СЕТИ;
- ЕСЛИ ВАС «ВЗЛОМАЛИ», НЕОБХОДИМО ПРЕДУПРЕДИТЬ ОБ ЭТОМ ВСЕХ ЗНАКОМЫХ;
- УСТАНОВИТЕ НАДЕЖНЫЙ ПАРОЛЬ (PIN) НА МОБИЛЬНЫЙ ТЕЛЕФОН;
- ОТКЛЮЧИТЕ СОХРАНЕНИЕ ПАРОЛЯ В БРАУЗЕРЕ;
- НЕ ОТКРЫВАЙТЕ ФАЙЛЫ И ДРУГИЕ ВЛОЖЕНИЯ В ПИСЬМАХ, ДАЖЕ ЕСЛИ ОНИ ПРИШЛИ ОТ ДРУЗЕЙ.