Профилактика киберпреступлений

Сеть Интернет стала практически незаменимым средством повседневной связи и обмена информацией по всему миру, и преступники не могут этим не пользоваться. Два миллиарда пользователей Интернета по всему миру создают идеальную среду для совершения преступлений, где можно действовать анонимно и получать доступ к любой персональной информации, которую мы, желая того или нет, размещаем в сети. В последние годы безопасность в сети Интернет подвергается более серьезным угрозам, и от преступлений в глобальном киберпространстве страдают более 431 миллиона взрослых пользователей.

Правила информационной безопасности:

НЕОБХОДИМО: создавать персональные (уникальные) пароли к разным сервисам; использовать сложные пароли: минимум 10 символов, одновременно цифры, строчные и прописные символы, знаки пунктуации и другие символы; доверять только проверенным менеджерам паролей

НЕ РЕКОМЕНДУЕТСЯ: использовать повторения символов; хранить пароли на бумажном носителе; использовать в качестве пароля свой логин; сохранять пароли автоматически в браузере; использовать биографическую информацию в пароле.

БЕЗОПАСНЫЙ Wi-Fi

НЕОБХОДИМО: отключить общий доступ к своей Wi-Fi точке, даже если у вас "безлимитный" интернет; использовать надежный пароль для доступа к вашей Wi-Fi точке; деактивировать автоматическое подключение своих устройств к открытым Wi-Fi точкам.

НЕ РЕКОМЕНДУЕТСЯ: вводить свой логин и пароль доступа к учетной записи (странице) или системе банковского обслуживания при подключении к бесплатным (открытым) точкам Wi-Fi в кафе, транспорте, торговых центрах и т.д.

ПРОВЕРЕННЫЕ БРАУЗЕРЫ И САЙТЫ

НЕОБХОДИМО: использовать специальное программное обеспечение (антивирус, расширение для браузера), чтобы избежать посещения сомнительных сайтов.

НЕ РЕКОМЕНДУЕТСЯ: переходить по непроверенным ссылкам; вводить информацию на сайтах, если соединение не защищено (нет https)

БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПОЧТЫ

НЕОБХОДИМО: подключать двухфакторную аутентификацию; использовать минимум 2 типа e-mail адресов: закрытый (только для привязки устройств и средств их защиты) и открытый (для переписки, подписок и т.д.); использовать СПАМ-фильтры.

НЕ РЕКОМЕНДУЕТСЯ: реагировать на письма от неизвестных отправителей: скорее всего это спам или мошенники; открывать подозрительное вложение к письму: сначала позвоните отправителю и узнайте, что это за файл.

ИСПОЛЬЗОВАНИЕ ПРИЛОЖЕНИЙ, СОЦСЕТЕЙ И МЕССЕНДЖЕРОВ

НЕОБХОДИМО: устанавливать приложения только из PlayMarket, AppStore или из проверенных источников; обращать внимание, к каким функциям гаджета приложение запрашивает доступ; обмениваться сообщениями в

соцсетях и мессенджерах, только полностью удостоверившись в личности собеседника, не реагируя на сомнительные просьбы и предложения.

НЕ РЕКОМЕНДУЕТСЯ: размещать персональную и контактную информацию о себе в открытом доступе; использовать указание геолокации на фото в постах; отвечать на обидные выражения и агрессию в соцсетях - лучше напишите об этом администратору ресурса; употреблять ненормативную лексику при общении.

ЗАЩИТА БАНКОВСКИХ КАРТОЧЕК

НЕОБХОДИМО: Хранить в тайне пин-код карты; прикрывать ладонью клавиатуру при вводе пин-кода; оформить отдельную карту для онлайн покупок и не держать на ней большие суммы; использовать услугу 3-D Secure и лимиты на максимальную сумму онлайн-операций; скрыть CVV-код на карте (трехзначный номер на обратной стороне), предварительно сохранив его.

НЕ РЕКОМЕНДУЕТСЯ: хранить пин-код вместе с карточкой/на карточке; сообщать CVV-код или отправлять его фото; распространять свои паспортные данные (информацию личного характера, номер мобильного телефона), «логин» и «пароль» доступа к системе «Интернет – банкинг»; сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации, пароли 3-D Secure.