Профилактика преступлений с использованием IT-технологий

Безопасность в цифровом пространстве имеет первостепенное значение в современном мире. Эта памятка поможет вам защититься от различных киберугроз и сохранить конфиденциальность ваших данных.

Виды киберпреступлений

1

Фишинг

Мошенничество с целью кражи личной информации через поддельные сайты и письма.

2

Вирусные атаки

Заражение устройств вредоносным программным обеспечением для кражи данных или парализации работы.

3

Кража личных данных

Незаконное получение и использование частной информации для мошеннических целей.

Меры личной безопасности

Осторожность в Интернете

Будьте бдительны при просмотре веб-сайтов, открытии писем и установке приложений.

Безопасность паролей

Используйте надежные, уникальные пароли для каждого аккаунта и включите двухфакторную аутентификацию.

Защита устройств

Регулярно обновляйте программное обеспечение и устанавливайте антивирусные решения на свои устройства.

Осторожность в соцсетях

Будьте внимательны к публикуемому контенту и ограничивайте доступ к личной информации.

Безопасность аккаунтов и паролей

Сложные пароли

Используйте длинные, уникальные пароли, содержащие буквы, цифры и специальные символы.

Двухфакторная аутентификация

Включите двухфакторную аутентификацию для дополнительной защиты учетных записей.

Управление паролями

Используйте надежный менеджер паролей, чтобы генерировать и хранить ваши учетные данные.

Безопасность онлайн-транзакций

1 Проверка сайтов

Убедитесь, что сайты, на которых вы совершаете покупки, имеют HTTPS-протокол и надежную репутацию.

2 Использование карт

Отдавайте предпочтение кредитным картам, так как они предоставляют больше защиты от мошенничества.

3 Мониторинг действий

Регулярно проверяйте выписки по счетам и отчеты о транзакциях на предмет подозрительной активности.

Установка антивирусов

Используйте надежные антивирусные программы для защиты ваших устройств от вредоносных программ.

Обновление ПО

Своевременно обновляйте операционные системы и приложения для устранения уязвимостей.

Защита устройств

Шифрование данных

Включите шифрование данных на своих устройствах, чтобы защитить конфиденциальную информацию.

Резервное копирование

Регулярно создавайте резервные копии важных данных на внешних носителях или в облаке.

Осторожность в социальных сетях

Ограничение доступа

Настройте профили в социальных сетях на максимальную конфиденциальность, чтобы ограничить доступ к личной информации.

Осторожность при публикациях

Тщательно продумывайте содержание и аудиторию ваших публикаций, чтобы избежать раскрытия личных данных.

Двухфакторная аутентификация

Включите двухфакторную аутентификацию на ваших аккаунтах в социальных сетях для дополнительной защиты.

Осторожность при получении сообщений

1

Проверка отправителя

Убедитесь, что сообщение действительно пришло от надежного источника, прежде чем открывать его.

2

Осторожность с ссылками

Не переходите по ссылкам в подозрительных сообщениях, так как они могут быть использованы для кибератак.

3

Избегайте пересылки

Не пересылайте сомнительные сообщения другим, чтобы не распространять возможную угрозу.

Действия при киберинцидентах

Защита данных

Предпримите меры для защиты своих учетных записей и устройств.

Сбор доказательств

Сохраняйте все документы, связанные с киберинцидентом, для последующего расследования.

Реагирование

Немедленно отреагируйте на подозрительную активность или кражу личных данных.

Обращение в службы

Свяжитесь с соответствующими государственными органами для расследования инцидента.