Памятка по профилактике преступлений, совершаемых с использованием информационно-телекоммуникационных технологий

1. Основные виды преступлений

К распространённым преступлениям в сфере ИКТ относятся:

- фишинг (попытки получения конфиденциальных данных через поддельные сайты и письма);
- мошенничество с использованием социальных сетей и мессенджеров;
- звонки от лжебанков и лжеполицейских;
- распространение вредоносного ПО (вирусов, троянов, программ-вымогателей);
- кража учётных записей и личных данных;
- инвестиционные и финансовые пирамиды в интернете;
- фейковые онлайн-магазины и аукционы.

2. Признаки подозрительных действий

Будьте бдительны, если:

- вам предлагают «выгодный» заработок без усилий или гарантированную высокую доходность инвестиций;
- просят срочно перевести деньги, ссылаясь на чрезвычайную ситуацию с близким человеком;
- сообщают о «блокировке счёта» или «подозрительной операции» и просят назвать код из SMS, данные карты или логины/пароли;
- присылают ссылки на сайты, похожие на официальные, но с небольшими отличиями в адресе;
- требуют установить приложение из непроверенного источника или открыть подозрительный файл;
- собеседник давит на эмоции (страх, жадность, срочность), не давая времени на обдумывание;
- предлагают оплатить товар или услугу на личную карту физлица без договора.

3. Правила безопасности

Для защиты устройств:

- установите антивирусное ПО и регулярно обновляйте его;
- обновляйте операционную систему и приложения до последних версий;
- используйте сложные и уникальные пароли для каждого сервиса (длина от 12 символов, сочетание букв, цифр, спецсимволов);
- включите двухфакторную аутентификацию (2FA) везде, где это возможно;
- отключите автозапуск USB-устройств и проверяйте флешки антивирусом перед использованием.

При работе в сети:

- не переходите по ссылкам из писем и сообщений от незнакомых отправителей;
- проверяйте адрес сайта в браузере: он должен начинаться с `https://` и иметь значок замка;
- не публикуйте в соцсетях личные данные (номер телефона, адрес, фото документов);
- будьте осторожны с приложениями, запрашивающими избыточные разрешения (доступ к контактам, камере, микрофону);
- при подключении к публичным Wi-Fi сетям убедитесь в их безопасности.

При финансовых операциях:

- никогда не сообщайте CVV/CVC-код, PIN-код и коды из SMS третьим лицам (в т.ч. «сотрудникам банка»);
- проверяйте реквизиты получателя перед переводом, особенно если сумма крупная;
- пользуйтесь только официальными приложениями банков и платёжных систем;
- установите лимиты на операции по картам;
- регулярно проверяйте выписки по счетам на предмет подозрительных транзакций.

4. Что делать, если вы стали жертвой преступления

1. **Немедленно прекратите общение** с мошенником.
2. **Заблокируйте карту** через мобильное приложение банка или по телефону горячей линии.
3. **Сообщите в банк** о подозрительной операции — возможно, транзакцию удастся отменить.
4. **Напишите заявление в полицию**:
    - лично в отделении;
    - онлайн через сайт МВД (раздел «Приём обращений»).
5. **Сообщите о мошенничестве** на горячую линию поддержки банка или платёжной системы.
6. **Сохраните доказательства**: скриншоты переписки, записи звонков, чеки, номера телефонов и адреса электронной почты мошенников.

5. Полезные контакты

- **Полиция**: 102 или 112 (экстренный вызов);
- **Банк России**: горячая линия по вопросам кибербезопасности (контакты на официальном сайте);
- **Портал «Госуслуги»**: раздел «Сообщить о мошенничестве»;
- **Сайты банков**: разделы «Безопасность» и «Горячая линия».

Важно! Будьте критичны к любой информации в сети. Если предложение кажется слишком выгодным, скорее всего, это обман. Перепроверяйте факты через официальные источники и консультируйтесь с близкими.