Памятка
по противодействию мошенничеству
с использованием информационно-коммуникационных технологий (ИКТ)

Что такое мошенничество с использованием ИКТ

Это действия злоумышленников с использованием интернета, телефона, мессенджеров и других средств связи с целью завладеть деньгами или персональными данными.

Типичные схемы мошенничества

- **От имени госорганов и организаций** — звонки или сообщения «из банка», «из суда», «из полиции», «из Минкультуры», «из РУМЦ» с требованием перевести деньги, назвать данные карты или пароли.
- **Фишинг** — письма и ссылки, имитирующие официальные сайты и сервисы, для кражи логинов, паролей и данных карт.
- **Социальная инженерия** — просьбы «срочно» перевести деньги, помочь «родственнику» или «руководителю», пройти по ссылке или установить программу.

Как защититься

1. **Не переводите деньги** по просьбе незнакомых людей по телефону, в мессенджерах или по ссылкам из писем.
2. **Не сообщайте** коды из SMS, данные карты (номер, срок, CVC), пароли от банка и госуслуг по телефону или в переписке.
3. **Проверяйте источник**: официальные запросы от организаций приходят по известным каналам. При сомнении позвоните в организацию по номеру с её официального сайта.
4. **Не переходите по подозрительным ссылкам** из писем и сообщений и не устанавливайте программы по просьбе неизвестных лиц.
5. **Используйте сложные пароли** и по возможности двухфакторную аутентификацию в важных сервисах.

Что делать при подозрении на мошенничество

- Прекратите общение и не выполняйте требования (переводы, передача данных, кодов, паролей, установка программ).
- Сообщите о произошедшем руководителю и, при необходимости, в правоохранительные органы (полиция, отдел по борьбе с киберпреступностью).
- При переведённых деньгах — сразу обратиться в банк и в полицию.

Контакты для обращения

- Полиция: **102** или **112**
- Официальный сайт МВД России и разделы по кибермошенничеству — для подачи заявления и получения актуальной информации.