

Если вас обманули по телефону: краткий алгоритм действий

На территории Могилевской области в текущем году наблюдается снижение количества зарегистрированных киберпреступлений.

Проводимая широкомасштабная воспитательно-профилактическая работа с населением в целом позволила несколько стабилизировать криминогенную обстановку в сфере противодействия киберпреступности на территории Могилевской области. Несмотря на это, необходимо понимать, какие действия следует предпринять при общении с мошенниками.

Прекратите контакт. Немедленно завершите разговор и заблокируйте номер. Любые «проверки», «возвраты» и «секретные операции» – продолжение мошенничества.

Срочно свяжитесь с банком. Позвоните по официальному номеру. Попросите охлаждение транзакций, отмену/оспаривание операций, блокировку карт и доступа, смену лимитов и паролей.

Если деньги передали курьеру или наличными. Немедленно обращайтесь в милицию. Максимально подробно опишите курьера, место и время передачи, возможные камеры и маршрут.

Предупредите близких. Если вы лишились доступа к аккаунтам или есть риск подмены, сразу сообщите родственникам и коллегам – мошенники могут писать и звонить от вашего имени.

Сохраните доказательства. Ничего не удаляйте: переписки, записи, звонков, смс-сообщения, уведомления банка. Сделайте скриншоты, зафиксируйте номера, ссылки, реквизиты, даты и время.

Важно: требования «удалить переписку», «установить приложение» или «никому не говорить» – стандартный признак мошенничества. Сохранение данных – ключ к защите и расследованию.

Проверьте устройство и аккаунты. Удалите подозрительные приложения, отзовите разрешения, смените пароли (банк, почта, соцсети), включите двухфакторную аутентификацию.

Подайте заявление. Лично обратитесь в территориальные органы внутренних дел, приложите все материалы. Это важно и для установления причастных, и для последующих юридических действий.

ОИОС по материалам КПК УМ УВД