**Новая схема обмана в сети: как ее распознать и что делать?**

В последнее время участились случаи, когда мошенники представляются сотрудниками мобильного оператора «МТС». Под выдуманными предлогами (необходимость продления договора, страхование или декларирование денежных средств) они предлагают установить приложение удаленного доступа «Мой МТС.арк», а получив доступ к мобильному устройству похищают с карт-счета сбережения доверчивых граждан.

**Запомните:** установив фейковое приложение, вы тем самым даете мошенникам доступ к своим данным, включая логины и пароли. Это позволяет преступникам свободно получать информацию о банковских счетах, личной переписке и других конфиденциальных сведениях!

Так, пенсионерка из Круглого, установив приложение «Мой МТС», после общения с лже-оператором сотовой сети, лишилась более 1 000 рублей, а жительница Кричева, спасая свои сбережения, пополнила банковский счет и сообщила мошенника логин и пароль от М-банкинга, потеряв около 15 000 рублей.

**Чтобы не стать жертвой киберзлоумышленников следуйте простым правилам:**

* сотрудники мобильных операторов не звонят абонентам через мессенджеры и не используют номера иностранных операторов, а также никогда не требуют изменить пароли под диктовку;

-договоры с компанией МТС заключаются на бессрочной основе и продлеваются автоматически;

-если вы получаете звонок через любой мессенджер с неизвестного номера, не передавайте личные данные, прервите разговор и обратитесь в официальный контактный центр МТС (0890) для проверки информации;

* приложение «Мой МТС» можно скачать только из официальных магазинов Google Play. Арр Store и Арр Gallery;

никогда не устанавливайте приложение по ссылкам, полученным от неизвестных источников через мессенджеры ил присланные в виде АРК- файла.

**По материалам УПК УВД Могилевского облисполкома**