**Как защитить себя от кибермошенничества**

Кибермошенники постоянно совершенствуют методы обмана, используя новые технологии и социальную инженерию, поэтому необходимо быть в курсе актуальных схем. Ниже представлены наиболее распространенные сценарии мошенничеств и рекомендации по профилактике.

1. ***Совершение мошеннических действий под видом работников коммунальных служб и государственных органов.***

Злоумышленники выдают себя за сотрудников коммунальных служб (энергонадзора, водоканала, газовой службы), а также представителей правоохранительных органов, банков или других государственных структур. Они могут звонить по телефону, в том числе по стационарной линии, или использовать мессенджеры (Viber, Telegram, WhatsApp). Цель - под любым предлогом получить личные данные, реквизиты банковских карт или вынудить перевести деньги на «безопасные» счета. Macro работают в паре: один представляется сотрудником коммунальной службы, другой - правоохранительных органов или банка, убеждая жертву, что ее данные скомпрометированы и для «спасения» средств необходимо оформить кредит или перевести деньги.

Приведем примеры подобных преступлений, имевших место на территории Могилевщины.

Пенсионерка из Горок, 1944 г.р., заявила в милицию о том, что 19 июня неизвестный с использованием глобальной сети «Интернет» в мессенджере «Viber», представившись сотрудником Департамента финансовых расследований, под предлогом декларирования денежных средств, убедил установить приложение удаленного доступа мобильного оператора, после чего с ее банковского счета похитил 7500 рублей.

Жителю агрогородка Новые Самотевичи, 1958 г.р., в мессенджере «WhatsApp» также позвонил неизвестный и, представившись сотрудником правоохранительных органов, обманным путем, под предлогом сохранности денежных средств, похитил с его банковской карты 11900 рублей.

1. ***Мошенничества с использованием мобильной связи***

Злоумышленники представляются сотрудниками операторов сотовой связи (А1, МТС). Под предлогом окончания срока действия договора или необходимости обновления услуг они убеждают жертву перейти по ссылке из мессенджера и скачать поддельное приложение. Последнее дает злоумышленникам полный доступ к данным на смартфоне, включая коды из SMS, логины и пароли к онлайн-банкингу.

и

Важно помнить: безопасное скачивание приложений возможно только из официальных магазинов, таких как Google Play, Арр Store, Арр Gallery. Никогда не устанавливайте приложения, переходя по сомнительным ссылкам.

С пенсионеркой из Могилева, 1949 г.р., неизвестный связался посредством мессенджера «WhatsApp». Представился сотрудником одной из мобильных кампаний и под предлогом продления договора об оказании услуг, посредством неустановленной фишинговой ссылки программного обеспечения мобильного оператора, с карт-счета женщины похитил 6000 рублей.

Жительница агрогородка Махово Могилевского района, 1949 г.р., также попала на уловку мошенника. В июне неизвестный с использованием глобальной сети «Интернет» в мессенджерах «Viber» и «WhatsApp» позвонил пенсионерке и, представившись сотрудником мобильного оператора и правоохранительных органов, под предлогом смены тарифного плана и продления договора об оказании услуг, убедил сообщить реквизиты ее банковской карты и коды, приходящие по СМС. После этого с указанного карт-счега похитил более 2600 рублей.

Во всех перечисленных случаях следователями возбуждены уголовные дела.

По материалам УПК УВД Могилевского облисполкома