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 распространённые сценарии мошенничести 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 так же представителей правоохранительных органов, банков или других государственных структур. Они могу 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. Часто работают в паре: один представляется сотрудником коммунальной службы, другой – правоохранительных органов или банка, убеждая жертву, что её данные скомпрометированы и для «спасения» средств необходимо оформить кредит или перевести деньги.

Приведём примеры подобных преступлений, имевших место на территории Могилевщины.

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

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

2. Мошенничества с использованием мобильной связи

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

Важно помнить: безопасное скачивание приложений возможно только из официальных магазинов, таких как Google Play, App Store, App 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 компаний и под предлогом продления договора об оказании услуг, посредством неустановленной фишинговой ссылки программного обеспечения мобильного оператора, с карт-счёта женщины похитили 6000 рублей.

Жительница агрогородка Махово Могилёвского 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 её банковской карты и коды, приходящие по СМС. После этого с указанного карт-счёта похитили более 2600 рублей.

Во всех перечисленных случаях следователями возбуждены уголовные дела.

По материалам УПК УВД Могилевского облисполкома.