Профилактика мошенничества в сети Интернет

На территории Республики Беларусь продолжают совершаться мошеннические действия в отношении граждан. В настоящее время основными способами завладения денежными средствами граждан являются фишинг и вишинг:

ФИШИНГ: В последнее время вызывает озабоченность рост преступлений методом фишинга – способа, цель которого – завладеть личными данными: реквизитами банковских платежных карт, сеансовыми ключами (кодами из смс), паролями к сервисам, чаще всего к М-банкингу. Мошенники умело подделывают различные интернет-ресурсы, которые имеют услугу онлайн-платежей, например, банковские услуги, торговые площадки, службы доставки и другие.

ВИШИНГ: Мошенники чаще всего используют для совершения преступлений звонки в мессенджерах. Звонящие могут представиться сотрудниками банковских организаций или правоохранительных органов. Под различными предлогами они убеждают произвести какие-либо действия, например, передать конфиденциальную информацию, в том числе смс-коды, оформить кредит или установить мобильное приложение.

При осуществлении мошеннических действий злоумышленники в основном используют мессенджеры такие как: «Whatsapp», «Telegram», «Viber».

ОБЩИЕ РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ОТ КИБЕРПРЕСТУПНИКОВ

- **Никому ни под каким предлогом не передавать номер банковской карты, срок действия, трехзначный секретный код на обороте, логины и пароли доступа к банкингу, смс-коды от банка.**
- **Не устанавливать программы и не переводить деньги по указанию, полученному по телефону даже от работников банка или милиции.**
- **При поступлении звонка в мессенджере от работника банка, закончить разговор и перезвонить в банк самостоятельно.**
- **При онлайн-оплате, в том числе услуг такси, проверять адрес сайта и использовать отдельную карту (виртуальную), хранить на ней небольшие суммы.**

Вриод начальника Берестовицкого РОВД Лозовицкий О.С.