Как не стать жертвой киберпреступлений

Достижения науки и техники, создание всемирной сети интернет позволили преступности выйти на новый уровень и захватить киберпространство.

Теперь преступнику не нужен прямой контакт с жертвой, он может стать угрозой для каждого пользователя «глобальной паутины», крупных корпораций и целых государств.

Защита пожилых людей от мошенников — это постоянный процесс. Чем больше вы будете общаться и информировать их, тем меньше шансов, что они станут жертвами обмана. Мошенники постоянно совершенствуют схемы обмана, поэтому наша задача — не просто предупредить, а научить человека моментально распознавать угрозу.

Лучшая защита — это бдительность и знание простых правил: никаких кодов из СМС, никаких «безопасных счетов», только личный визит в банк и звонки правоохранителям.

Мошенники постоянно придумывают новые способы обмана, и пожилые люди часто поддаются на их уловки. Поговорите с ними о мошенничестве. Объясняйте, какие схемы сейчас популярны и расскажите реальные истории о тех, кто попался на удочку мошенников.

Основные схемы мошенничеств:

«Оператор сотовой связи» и «Белтелеком». В ходе беседы злоумышленник сообщает человеку, что у него заканчивается срок действия договора на оказание услуг. Путем оформления заявки мошенники узнают паспортные данные и склоняют к установке сторонних приложений.

«Обновление кода домофона». Мошенник звонит жертве, представляясь сотрудником управляющей компании, службы безопасности или другой официальной организации. Злоумышленники сообщают, что новый код придет в СМС и его надо сообщить для обновления в системе. Только на самом деле СМС поступает от банка для получения кредитов, где получателями денежных средств являются злоумышленники.

«Водоканал» и «Электросети»: проверка или замена счетчиков. В ходе беседы злоумышленник предлагает человеку оставить заявку на поверку или замену счетчиков. Используя легенду о необходимости заполнения заявки, злоумышленники выманивают конфиденциальные паспортные данные. Следует отметить, что злоумышленники активно используют как мессенджеры, так и домашние телефоны для осуществления указанных схем преступлений.

«Декларирование денежных средств с целью их сохранности». Мошенник убеждает потерпевшего сообщить поступивший из СМС код. Затем поступает второй звонок, где неизвестный угрожает возбуждением

уголовного дел, проведением по месту жительства обыска, в ходе которого все денежные средства будут изъяты и предлагает во избежание этого сбережения передать «курьеру» для декларирования и сохранности. Не единичны случаи, когда в роли курьеров мошенники используют лиц, ранее обманутых аферистами и убеждают в том, что они участвуют в проводимой правоохранительными органами спецоперации.

Необходимо на постоянной основе доводить до сведения населения, особенно пожилым и престарелым, что:

Сотрудники милиции и иных правоохранительных органов никогда не звонят в мессенджерах и не требуют перевода денег для «декларирования» или «освобождения от ответственности»!

Никому нельзя сообщать свои личные данные, данные банковских карт, коды из SMS по телефону, даже если звонящий говорит, что он из банка или другой организации!

Ни при каких обстоятельствах нельзя оформлять кредиты по просьбе третьих лиц и переводить денежные средства на неизвестные банковские «безопасные» счета!

Нельзя открывать электронные письма от незнакомцев и переходить на подозрительные ссылки!

С целью повышения цифровой грамотности населения (в том числе с целью профилактики преступлений в отношении пожилых и престарелых граждан) и профилактики киберпреступлений в Брестской области, функционирует телеграм-канал «КИБЕРКРЕПОСТЬ», администрируемый управлением по противодействию киберпреступности УВД.

В связи с вышеизложенным, всем сотрудникам, в том числе и гражданскому персоналу рекомендуем подписаться на телеграм-канал «КИБЕРКРЕПОСТЬ».

С целью охвата всех слоев населения, профилактики киберпреступлений в рамках проведения бесед в трудовых коллективах организаций, предприятий и учреждений, учебных заведениях, предлагать подписаться на телеграм-канал «КИБЕРКРЕПОСТЬ» и иные Интернет-ресурсы УВД для получения актуальной и оперативной информации о совершаемых киберпреступлениях и способах противодействия таким преступлениям.

Осуществить подписку на вышеуказанный телеграм-канал можно с использованием QR-кода, а также путем введения в поисковую строку мессенджера «Telegram» «КИБЕРКРЕПОСТЬ».

УОПП УВД Брестского облисполкома