Внимание, новая схема вишинга!

Мошенники могут представляться сотрудниками правоохранительных органов или госучреждений

В Беларуси по-прежнему острой остается проблема совершения хищений денежных средств со счетов белорусов мошенниками, под видом «лжебанкиров» звонящих на телефоны белорусов и выведывающих конфиденциальную информацию. С начала года рост такого вида киберпреступлений составил свыше 220% (по сравнению с аналогичным периодом прошлого года).

Киберпреступники регулярно видоизменяют свои преступные схемы. На днях в Беларуси зафиксирована обновленная схема вишинга, жертвами которой уже стали двое жителей Гомельской и Могилевской областей. В обоих случаях мошенники для введения жертв в заблуждение действовали от имени якобы сотрудников правоохранительных органов.

Так, на днях жителю Могилева на телефон поступил звонок от неизвестного, который представился руководителем одного из подразделений УВД Могилевского облисполкома. Он сообщил, что банковский счет мужчины скомпрометирован, проводятся оперативно-розыскные мероприятия по установлению подозреваемого. Для успешной операции, мол, от владельца необходимо получить определенную информацию о счете и совершить ряд действий для обеспечения его безопасности. Мужчина, не удосужившись проверить достоверность озвученной незнакомцем информации, легкомысленно снял с депозитного счета $3 тысячи и перевел их на его счет.

Схожий случай произошел вчера в Гомеле. Неизвестный позвонил местной жительнице по «Вайберу», представился сотрудником банка и сообщил, что ее банковский счет находится под угрозой. Также сообщил, что расследованием якобы занимается один из руководителей УВД Минской области, озвучив при этом его должность, ФИО, номер мобильного телефона. В процессе диалога женщина беспрекословно выполняла требования мошенника: устанавливала на своем телефоне программу «AnyDesk», с помощью которой мошенник отслеживал и контролировал все ее действия; выведал конфиденциальную информацию к банковскому счёту; вынудил оформить и переоформить кредит. Таким образом, в результате мошеннических действий женщина лишилась около 15 тысяч рублей.

МВД предупреждает!

Вишинг-атаки совершаются методом социального инжиниринга. Нападающий создаёт критическую ситуацию, позволяющую эксплуатировать человеческие чувства, и убеждает жертву раскрыть ценную информацию. Мошенники используют фактор неожиданности и создают для жертвы

максимально неудобные условия при нехватке времени на анализ происходящего. Обычно их интересует номер банковской платежной карты, логин и пароль от кабинета пользователя, коды из sms-сообщения.

Чтобы не стать жертвой преступника, строго следуете основным правилам цифровой безопасности.

1. Помните, что по телефону собеседник может представляться кем угодно. Поэтому никогда не сообщайте незнакомым людям конфиденциальные данные. Кем бы они ни представлялись, как бы убедительно ни звучали их просьбы. Запомните: сотрудники банков или госучреждений никогда не будут у вас спрашивать данные, к которым у них и без того есть доступ!

2. Не устанавливайте на свой мобильный телефон какие-либо программы по просьбе неизвестных вам людей, и не предоставляйте им доступ к ранее установленным.

3. Обезопасьте свой основной банковский счет! Для совершения онлайн-платежей откройте в том же банке другой счет, который сможете пополнять при необходимости. И если даже этот счет будет скомпрометирован, ваш основной останется в безопасности.