

ВИШИНГОВАЯ АТАКА, ОДИН ИЗ СПОСОБОВ СОВЕРШЕНИЯ ХИЩЕНИЯ ДЕНЕЖНЫХ СРЕДСТВ С БАНКОВСКИХ СЧЕТОВ

Вишинг – способ мошенничества с помощью телефона, когда мошенник под различным предлогом пытается выманить персональную информацию жертвы для последующего хищения денег с ее банковского счета.

В Республики Беларусь уже зафиксированы случаи совершения хищения денежных средств со счетов белорусов мошенниками, которые под видом «лжебанкиров» звонят на телефоны белорусов и выведывают конфиденциальную информацию.

Однако киберпреступники регулярно видоизменяют свои преступные схемы. И как следствие, на днях в Республике Беларусь 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.



Сотрудники Министерства внутренних дел Республики Беларусь предупреждают!

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.

Таким образом, чтобы не стать жертвой киберпреступника, необходимо соблюдать следующие правила цифровой безопасности:

- необходимо помнить, что по телефону собеседник может представляться кем угодно. Поэтому будьте бдительны и 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!

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

- 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.