ИНФОРМАЦИЯ ДЛЯ КЛИЕНТОВ

О мерах по обеспечению информационной безопасности и противодействию мошенничества

Уважаемые Клиенты!

ПАО «НИКО-БАНК» информирует Вас об активизации мошеннических действий, направленных на проведение целевых атак на юридических лиц, являющихся клиентами кредитных организаций, с использованием вредоносного программного обеспечения с последующим осуществлением несанкционированных переводов денежных средств с их счетов.

Хищения средств со счетов юридических лиц, как правило, осуществляются в особо крупных размерах!

Настоятельно рекомендуем Вам проводить следующие мероприятия, направленные на повышение уровня защищенности объектов Вашей информационной инфраструктуры:

- использование решений для мониторинга и выявления киберугроз и оперативного реагирования на инциденты (MDR-решений);

- с помощью аппаратных или программных средств сетевой защиты (Firewall, корпоративные прокси-серверы) ограничить доступ в сеть «Интернет». Маршрутизировать трафик таким образом, чтобы разрешать соединения только с доверенными ресурсами;

- не допускать использования работниками организации рабочих устройств для личного использования, в том числе посещения развлекательных ресурсов, личной электронной почты или общения в мессенджерах;

- соблюдать требования безопасности при эксплуатации ключевого носителя (USB-токена), производить его извлечение из USB-порта сразу после подписания платежных поручений.

При выявлении инцидента информационной безопасности рекомендуем Вам выполнять следующие действия:

- не перезагружать компьютер, не запускать антивирусные решения, извлечь токены доступа (при их наличии) и съемные носители информации;

- отключить устройство от локальной сети и сети Интернет;

- выполнить процедуры создания образов оперативной памяти и жесткого диска с использованием специализированного программного обеспечения (например, «FTK Imager») для дальнейшего проведения расследования;

- при наличии возможности сохранить образец вредоносного программного обеспечения для проведения анализа и последующей передачи его в Банк (в рамках анализа компьютерного инцидента);

- в случае заражения мобильного устройства, необходимо включить авиа-режим и извлечь SIM-карту. Если в устройстве используется электронная сим-карта, допустимо выключить устройство. Сбрасывать устройство до заводских настроек не рекомендуется, так как это приведет к удалению следов вредоносной активности и затруднит дальнейшее проведение расследования.

Обращаем Ваше внимание**,** что выполнение мер по снижению рисков несанкционированного доступа, а также рекомендаций по обеспечению информационной безопасности при использовании системы ДБО на компьютере и мобильном устройстве размещенных на сайте ПАО «НИКО-БАНК», а также направляемых периодически в информационных рассылках, поможет защитить Ваши финансы и обеспечить безопасную работу с системой ДБО.