МВД Беларуси – об актуальных способах совершения киберпреступлений

Электронные сервисы, интернет-банкинг, удаленная работа и учеба, социальные сети, интернет-магазины и маркетплейсы – все это настолько прочно вошло в нашу повседневность, что иногда трудно представить, как мы жили без этого раньше. Чем больше погружаемся в мир информационно-коммуникационных технологий, тем уязвимее становимся для интернет-преступников.

Киберпреступность не стоит на месте, а активно идет в ногу со временем, с развитием технологий меняются схемы и способы обмана. Отдельное беспокойство вызывает применение искусственного интеллекта в преступной деятельности.

МВД Республики Беларусь разработаны и представлены памятки, другая информация, которая поможет каждому уберечь себя и близких от опасности.

Наиболее распространенным способом интернет-хищения денежных средств является **телефонное мошенничество.** Аферисты представляются работниками банков, коммунальных служб, водоканала, энергонадзора, служб газа и связи, сотрудниками правоохранительных и государственных органов, даже вашими знакомыми и родственниками. Чтобы похитить деньги, мошенники под различными предлогами пытаются завладеть личными данными, включая коды из смс. Часто они действуют в паре. Например, первый под предлогом замены ключей от домофона выманивает числовой код из смс, а второй мошенник, представляясь правоохранителем, угрожает проведением обыска и изъятием денежных средств за передачу того самого кода.

Или другой пример. Один мошенник представляется руководителем вашей организации и пугает подозрением в экстремистской деятельности и проведением обыска, а другой от имени правоохранителя предлагает якобы помощь в решении данной проблемы: для этого нужно перевести деньги на «временный счет» или передать их курьеру.

Помните: никаких временных счетов не бывает и вернуть свои деньги с чужого счета невозможно.

Также мошенники используют и другие схемы обмана. Аферист по телефону представляется работником банка или предприятия связи (Белтелеком, А1, МТС) и убеждает обновить мобильное приложение, для чего необходимо скачать и установить на телефон поддельное приложение, направленное ссылкой или файлом (*.apk) в мессенджере. Часто такие фейковые приложения предоставляют удаленный доступ к устройству и мошенник «подсматривает» все, что происходит на экране. Иногда этого бывает достаточно, чтобы похитить деньги.

Нельзя выполнять никаких действий, связанных с финансами, по указанию незнакомых, кем бы они не представились.

Еще один из распространенных способов – фейковые интернет-магазины в социальных сетях.

Остерегайтесь подозрительно низких цен и не переводите предоплату за товар или услугу, выбирайте оплату наложенным платежом.

Прежде чем согласиться на покупку, проверьте наличие у продавца сайта в белорусском сегменте интернета и созвонитесь с ним по телефону. Тщательно проверяйте информацию о продавце.

Крупные хищения мошенники совершают с использованием поддельных инвестиционных или криптоплатформ. Размещая рекламу в Интернете, они могут использовать видео с известными людьми – политиками, спортсменами, даже блогерами, которые озвучены фразами, сгенерированными с помощью искусственного интеллекта. Например, на видео может быть известная телеведущая, которая в репортаже рассказывает о якобы новой возможности заработка, или заместитель министра дает интервью, что многие уже пользуются определенным ресурсом и получают деньги, хотя на самом деле все слова – это всего лишь результат работы нейросетей. С заинтересовавшимися связываются так называемые кураторы или брокеры и убеждают участвовать в инвестировании или программе на том самом ресурсе. Для получения пассивного дохода предлагают вложить деньги в прибыльный проект. Часто жертв побуждают к оформлению кредитов для перевода большей суммы. На самом деле вкладчику просто «рисуют» его прибыль на сайте и никогда не дают возможности вывести его деньги.

Легких денег не бывает, а бесплатный сыр – в мышеловке. Вернуть деньги, «вложенные» подобным образом, невозможно.

Вымогательство за разблокировку Iphone – один из новых, набирающих обороты способов мошенничества. Используя его,аферист в переписке узнает у будущей жертвы о наличии Iphone, а потом под различными предлогами убеждает войти в его ICloud. Предлогами могут быть, например, помощь в восстановлении фотографий, сохранение диплома, возможность пройти уровень в игре или получить для своего героя игровое имущество, оружие или способность. После входа в ICloud мошенника, Iphone жертвы блокируется. Для его разблокировки предлагается заплатить сумму, в зависимости от модели, превышающую 1000 рублей.

Это не все, но самые актуальные и распространенные схемы, и со временем они могут меняться. Чтобы не стать жертвой киберпреступников, необходимо всегда адекватно оценивать свои действия и, как бы вас не запугивали, не поддаваться панике и страху. Будьте бдительны, берегите себя и свои деньги!

Больше информации по теме: