**Республиканская профилактическая акция «Неделя цифровой грамотности»**

С 26 ноября по 2 декабря МВД проведет республиканскую профилактическую акцию «Неделя цифровой грамотности».

Как сообщили в ведомстве, сотрудники милиции проведут комплекс мероприятий по повышению осведомленности населения о киберпреступлениях и способах защиты от них, формированию навыков безопасного поведения в интернете.

- Особое внимание уделят профилактике вовлечения несовершеннолетних в мошенническую деятельность и порядку осуществления операций с цифровыми знаками (токенами). Специалисты расскажут о распространенных видах киберпреступлений, в том числе совершаемых с использованием нейросетей, предупредят о современных способах интернет-афер и дадут практические советы по защите от них. Напомнят о правилах поведения в интернете, как не стать жертвой при покупке товаров, акцентируют внимание на распространении фейковых предложений об инвестировании в цифровую валюту, - отметили в МВД.

**ВИШИНГ**

**Вишинг** – один из методов мошенничества с использованием социальной инженерии. Он заключается в том, что злоумышленники, используя телефонную связь и выдавая себя за сотрудников банков (или правоохранителей, что особенно часто происходит в последнее время), под различными предлогами выясняют у потерпевших сведения о наличии банковских платежных карточек (далее – БПК), сроках их действия, CVV (CVC)-кодах, паспортных данных, смс-кодах с целью хищения денежных средств. В ряде случаев злоумышленникам известны некоторые реквизиты БПК, а также анкетные данные лиц, на имя которых они эмитированы.

В большинстве случаев при совершении звонков потерпевшим преступники используют IP-телефонию, которая позволяет маскировать телефонные номера под номера белорусских операторов связи. Кроме этого, зачастую злоумышленники используют мессенджеры Viber и WhatsApp, в которых существует возможность использования виртуальных номеров. Также преступники маскируются под логотипом узнаваемых белорусских банков, вводя в заблуждение потенциальных жертв.

Злоумышленники звонят жертве и от имени банковского сотрудника сообщают, что необходимо осуществить какие-либо действия с БПК, так как кто-то либо пытается похитить с нее денежные средства, либо оформляет кредит, либо производит подозрительную оплату. Завладев реквизитами карты, преступники осуществляют хищение денежных средств с банковского счета потерпевшего.

В последнее время наиболее актуальная схема – побуждение жертвы открыть кредит. Злоумышленники сообщают жертве о том, что якобы кто-то посторонний пытается открыть кредит на ее имя, и для его деактивации необходимо самостоятельно обратиться в банк и открыть кредит, переслав впоследствии реквизиты счета.

**ФИШИНГ**

**Фи́шинг** – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Фишинг используется для получения доступа к учетным записям пользователей самых различных ресурсов, но зачастую он применяется для хищения данных пользователей торговых онлайн-площадок.

Для этого злоумышленники подменяют страницу используемого жертвой интернет-сервиса на мошенническую, которая внешне является двойником оригинала. Фишинговая страница может иметь сходство с разными сервисами: Kufar, Белпочта, службой доставки, банками, ЕРИП и т. д. В соответствии с этим может использоваться разный предлог для перехода на страницу преступником (забрать зачисленные им деньги, подтвердить получение посылки на почте или в службе доставки, подтвердить прием средств на одном из банковских сервисов и т.д.).

Невнимательный интернет-пользователь может и не заметить подмены, так как подобные страницы визуально схожи с оформлением оригинальных сайтов. Когда пользователь заходит на такую поддельную страницу и вводит логин и пароль, они становятся доступны мошенникам.

**ФЕЙК АККАУНТ (НОВЫЙ ВИД)**

«фейк аккаунт (профиль)» в определенном интернет ресурсе.

Фейк аккаунт (профиль) – создан от чужого имени путем копирования реального человека: фамилия, имя, отчество, дата рождения, место жительства и иных сведений, присущих определенному человеку.

Данная форма мошеннических действий совершается следующим образом (пример):

- неустановленное лицо создает аккаунт (профиль) в мессенджере «Telegram» под поддельными данными присущими руководителю организации с установкой его фотографии полученной из сети Интернет.

- в последующем неустановленное лицо под именем руководителя организации предлагает сотрудникам организации, руководителем которой «он» является, получить те или иные услуги (совершить иные действия), выманивая денежные средства (паспортные/банковские данные); уведомляет о том, что с ними может связаться один из «руководителей» вышестоящей организации (который в свою очередь также предлагает получить те или иные услуги (совершить иные действия), выманивая денежные средства (паспортные/банковские данные).

Учитывая данный факт необходимо соблюдать следующее: при получении сообщения в сети «Интернет» от руководителя организации, в которой вы трудоустроены, коллег по работе, знакомых, друзей, родственников и иных лиц с просьбой оказания какой-либо услуги (совершения иных действий), необходимо – связаться с непосредственным отправителем сообщения посредством сотовой связи без использования «Интернет» ресурсов (Instagram, Telegram, Viber, WhatsApp, Skype, Одноклассники, ВКонтакте и др.) либо встретится лично, и удостовериться о факте отправки им данного сообщения.

**ЗВОНОК ОПЕРАТОРА СОТОВОЙ СВЯЗИ**

Данный способ мошенничества имеет следующий путь её реализации: поступает звонок от имени оператора «А1» (с любого мессенджера Telegram, Viber, WhatsApp и т.д). Неизвестный уведомляет о том, что заканчивается договор оформления Sim-карты, либо о том, что заканчивается кредитный договор/рассрочка на определенный товар, о необходимости обновления приложения на мобильном устройстве и т.д..

Далее события могут разворачиваться в нескольких направлениях: на мобильный телефон приходят SMS-сообщения c кодом доступа к профилю A1, которые неизвестный просит сообщить ему – в последствии чего неизвестный получает полный доступ к профилю абонентского номера приложения «Мой А1», в котором осуществляет заказы на различные товары в магазине «eShop»; неизвестный просит установить «якобы обновленное приложение А1», которое в действительности является приложением позволяющим получить удаленный доступ к определенному устройству, на которое оно было установлено, после чего неизвестный просит совершать определенные действия в устройстве (зайти в Интернет-банкинг и т.д.).

Учитывая тот факт, что все вышеуказанные способы на данный момент используются мошенниками для завладения денежными средствами граждан, необходимо строго соблюдать следующие рекомендации, чтобы не стать жертвой киберпреступника:

1. Не следовать инструкциям незнакомцев, позвонивших с неизвестного номера;
2. Не сообщать неизвестным лицам свои персональные данные;
3. Не совершать никаких действий на мобильном телефоне по просьбе посторонних лиц (скачивать и устанавливать различные приложения);
4. Не переводить деньги незнакомым людям в качестве предоплаты;
5. Не переходить по ссылке, полученной от неизвестных лиц- возможно она ведет на фишинговый сайт;
6. Не пользоваться открытыми вай-фай сетями в кафе или на улице;
7. Не реагировать на сообщения/письма от неизвестных отправителей;
8. Не открывать подозрительные вложения в письмах, поступивших Вам на электронную почту;
9. Не размещать персональную и контактную информацию о себе в открытом доступе;
10. Никому не сообщать CVV/CVC код на тыльной стороне банковской карты;
11. Не сообщать данные, полученные в виде СМС-сообщений, сеансовые пароли, коды авторизаций и т.д.;
12. Не сообщать кому-либо логин и пароль доступа к системе «Интернет-Банкинг»;
13. Не обращать внимания на обещания о внезапных выигрышах;
14. Не использовать одинаковые пароли для доступа к различным аккаунтам, учетным записям.

Данные правила помогут Вам сохранить Ваши денежные средства, хранящиеся на банковских счетах и не стать жертвой киберпреступника.