Памятка об актуальных способах совершения преступлений в Интернете

В настоящее время набирает актуальность следующий способы совершения преступлений в сети «Интернет»:

1) гражданину поступает звонок посредством различных мессенджеров («Вайбер», «Телеграмм», «WhatsApp») с различных абонентских номеров, в том числе и иностранных государств от мошенников, которые представляются сотрудниками правоохранительных органов, таких как КГБ, МВД, СК и сообщают, что расследуется «уголовное дело», в ходе расследования которого установлено, что Вы оказываете финансовую поддержку вооруженным силам Украины. Интересуются, сколько у Вас дома хранится денежных средств, в том числе в иностранной валюте. В последующем сообщают, что у Вас по месту жительства будет проведен обыск, в результате которого все денежные средства буду конфискованы. Иногда мошенники сообщают, что вышел новый закон, в соответствии с которым хранить дома денежные средства в иностранной валюте запрещено, в связи с чем их необходимо перевести на «сберегательный банковский счет», который принадлежит мошенникам. Вместе с этим мошенники сообщают, что необходимо установить на свой мобильный телефон специальное приложение (на самом деле обычное приложение для удаленного доступа к телефону), пример: «AnyDesk», «RustDesk». После чего необходимо проследовать в банк, зарегистрировать в нем БПК и уже непосредственно на нее зачислить денежные средства хранящиеся у вас дома. После этого мошенники дистанционно списывают деньги с вашей банковский карты.

2) Вторым наиболее актуальным способом интернет-мошенничества является:

Вам поступает звонок в мессенджерах «вайбер», «телеграмм», «WhatsApp» с иностранного номера, либо с номера Республики Беларусь якобы от сотрудников правоохранительных органов, либо от сотрудников безопасности Национального банка. Звонивший сообщает, что на Ваше имя неизвестный Вам гражданин оформляет кредит. В ходе беседы данное лицо присылает Вам «фотографию своего служебного удостоверения. Затем Вам сообщают о необходимости установки на мобильный телефон специального приложения (на самом деле обычное приложение для удаленного доступа к телефону, пример: «AnyDesk», «RustDesk»). После чего мошенник получает доступ к вашему телефону и похищает все имеющиеся у Вас денежные средства, находившиеся на Ваших банковских картах. Также вам могут сообщить, что задержан гражданин который подает заявку на оформление кредита от Вашего имени, после чего могут попросить оказать помощь в изобличении недобросовестных сотрудников банка и оформить на свое имя кредит, а денежные средства перевести на безопасный счет.

3) Следующим популярным способом интернет-мошенничества выступает создание так называемых «Интернет-магазинов» различной направленности. Например: продажа новогодних елок, мобильных телефонов,

кресел-коконов, одежды, обуви, иной мебели. Как правило, в данных интернет-магазинах устанавливаются «привлекательные» цены, увидев которые, граждане желают их приобрести. В ходе переписки с «администратором» данного торгового магазина, последний сообщает, что для приобретения товара необходимо внести предоплату. Чаще всего требуют 100% предоплату, но иногда требуют 50%. В любом случае после перечисления денежных средств никакой товар гражданину не поступает. Также как и не возвращаются денежные средства.

4) Актуальным способом интернет-мошенничества остаются мошеннические действия в сети «Интернет» под предлогом знакомств в таких социальных сетях как «Тикток», «Вконтакте», «Инстаграм», приложения для знакомств «Тиндер», «Дайвинчик». Здесь механизмов совершения мошеннических действий практически неограниченное количество. Обычно, злоумышленник (под видом красивой девушки или парня) осуществляет знакомство с жертвой и в ходе беседы сообщает, что он идет в театр/кино/иные заведения и предлагает вам приобрести билет на соседнее место. Для приобретения билета он сбрасывает поддельную ссылку на сайт театра/кинотеатра. Перейдя по данной ссылке, Вам необходимо ввести реквизиты своей БПК и подтверждающие смс-коды. После чего со счета вашей БПК похищаются денежные средства. Но это лишь один их механизмов. Еще одним способом хищения денежных средств, является якобы отправка подарка или денежных средств мошенником. Так, мошенник в ходе переписки сообщает, что на ваше имя планирует отправить подарки или денежные средства. Далее он сообщает, что отправил посылку, однако для ее доставки необходимо вносить различные оплаты. Как пример: оплата за доставку, за растаможку, за пересылку и иные платежи, которые иногда придумывает сам злоумышленник. Вместе с этим, имеет место способ, которому наиболее подвержены молодые парни. В приложении для знакомств привлекательная девушка знакомится с парнем и в ходе переписки просит его активировать якобы ее Icloud на мобильном телефоне жертвы. После активации Icloud, мошенник блокирует мобильный телефон жертвы и требует за его разблокировку денежные средства различного размера. В случае отсутствия перевода, мошенник не снимает блокировку телефона жертвы и он перестает функционировать.

5) Особое место в сфере интернет-мошенничеств занимают завладения денежными средствами граждан путем обмана и злоупотребления доверием под предлогом осуществления инвестиций на криптовалютных биржах. Механизм банален и прост. Будущему потерпевшему в различных мессенджерах звонят или пишут мошенники и предлагают ему осуществлять инвестиции на различных криптовалютных биржах. При этом, мошенники заблаговременно создают сайты якобы криптовалютных бирж и наполняют их содержимым (контент, положительные отзывы и т.д.). В ходе беседы, вам навязывают услуги «брокера», который «помогает» вам инвестировать денежные средства. После прохождения всех этапов регистрации (на сайте, в приложении криптовалютной биржи, иных приложениях) вы начинаете «инвестировать». В результате данных действий вам на первоначальном этапе даже дают вывести часть денежных средств в небольшом размере (до 100 долларов США). При этом, на сайте в вашем личном кабинете отображается, что там якобы баланс составляет

значительные суммы денежных средств. После небольших выводов, вас побуждают осуществлять более крупные инвестиции и уже после крупных вложений денежных средств, мошенники растворяются с деньгами и перестают выходить на связь. Одновременно с этим, на сайте, предложенном «брокером», баланс составляет большую сумму денежных средств, однако вывести их не получится.

Значительное количество взломов профилей в мессенджерах «Вайбер», «Телеграмм», «WhatsApp» случается из-за того, что граждане переходят по подозрительным ссылкам в данных мессенджерах.

6) Что касается предприятий и юридических лиц, то набирает популярность вариант обмана, когда на электронную почту скидывают письмо, содержащее вредоносный файл. После скачивания данного файла злоумышленник получает доступ к компьютеру организации, на котором чаще всего имеются важные рабочие документы и программы. Затем злоумышленник блокирует компьютер организации и требует за его разблокировку денежные средства. Также актуальным способом хищения денежных средств путем обмана и злоупотребления доверием остается способ, когда злоумышленник скидывает на электронную почту предприятия «очень выгодное предложение» о приобретении товаров или услуг по привлекательной цене. После перечисления денежных средств предприятием, ни услуга, ни товар в адрес заказчика не поступает. Денежные средства также никто не возвращает.

ИИ

1. Гражданам звонят мошенники, выдающие себя за правоохранителей, утверждая, что расследуется уголовное дело о финансовой поддержке вооруженных сил Украины. Они запугивают обыском и конфискацией денег, предлагая перевести их на банковский счет мошенников. Также требуют установить приложение для удаленного доступа и списывают деньги с банковской карты. Важно не поддаваться на подобные угрозы и быть бдительным.

2. Мошенники с использованием иностранных или белорусских номеров, представляясь правоохранителями или сотрудниками банка, уведомляют о вымышленном кредите. После предоставления фотографии удостоверения они требуют установить приложение для удаленного доступа (например, AnyDesk, RustDesk) и крадут деньги с ваших банковских карт. Могут также сообщать о задержании лица, подающего заявку на кредит от вашего имени, с просьбой помочь "изобличить" недобросовестных сотрудников, переведя деньги на "безопасный счет". Будьте осторожны и не поддавайтесь на уловки.

4. Интернет-мошенники создают фиктивные "Интернет-магазины" с разными товарами и привлекательными ценами, например, новогодние елки, мобильные телефоны, одежду. В переписке с "администратором" гражданам говорят о необходимости предоплаты (обычно 100% или 50%). После перечисления денег товар не поступает, и средства не возвращаются. Будьте внимательны при онлайн-покупках и избегайте подобных мошеннических схем.

5. В интернете продолжают действовать мошеннические схемы, связанные с фиктивными знакомствами в социальных сетях и приложениях знакомств. Злоумышленники, представляясь привлекательными собеседниками, предлагают покупку билетов на различные мероприятия через поддельные ссылки, заставляя вводить банковские реквизиты и смс-коды. Еще один метод - обещание отправить подарок или деньги, после чего требуют оплату за доставку, растаможку и другие вымышленные расходы. Для молодых парней применяется схема, где привлекательная девушка в приложении для знакомств просит активировать ее Icloud на мобильном телефоне, после чего блокирует устройство и требует денежное вознаграждение за разблокировку. Важно быть осторожными и избегать подобных мошеннических уловок в сети.

6. Мошенники в сфере интернет-мошенничества применяют обман и злоупотребление доверием, предлагая гражданам инвестировать на криптовалютных биржах. Они создают поддельные сайты криптовалютных бирж с контентом и положительными отзывами. Предлагают услуги "брокера", который помогает инвестировать средства. На первых этапах разрешают небольшие выводы, чтобы убедить вас в успешности инвестиций. После крупных вложений мошенники исчезают, переставая выходить на связь. Одновременно, на сайте баланс остается недоступным для вывода. Также отмечается взлом профилей в мессенджерах из-за перехода по подозрительным ссылкам. Будьте осторожны, избегайте подобных предложений и подозрительных ссылок.

7. В корпоративном обмане часто используется метод отправки вредоносного файла на электронную почту предприятий. После загрузки файла злоумышленник блокирует компьютер, требуя денежные средства за разблокировку. Еще один метод - отправка фиктивных предложений о покупке товаров или услуг по привлекательной цене на электронную почту предприятия. После оплаты ни товар, ни услуга не поступают, а деньги не возвращаются. Будьте бдительны в обращении с электронной почтой.