Профилактическая акция «Неделя цифровой грамотности»

Стремительное развитие цифровых технологий, переход к безналичным расчетам, размещение в глобальной компьютерной сети Интернет персональных данных при достаточно низкой цифровой грамотности граждан, сопряженной с беспечным отношением к защите собственной информации, стали следствием увеличения количества регистрируемых киберпреступлений.

Злоумышленники активно используют в своей деятельности новейшие достижения науки и техники, применяют всевозможные компьютерные устройства и новые информационные технологии для совершения и сокрытия преступлений.

По итогам десяти месяцев 2024 года, в сравнении с аналогичным периодом прошлого года (далее - АППГ), количество зарегистрированных киберпреступлений на территории Минской области увеличилось на **21,9% (с 1603 до 1954),** что является **каждым пятым (20,3%) уголовным делом на Минщине**. Число тяжких киберпреступлений возросло **в 0,8 раз (с 125 до 228 или на 82,4%)**.

Так в январе - октябре 2024 года на территории Минской области совершено **1123** мошенничества (ст. 209 Уголовного кодекса) или **57,5%** от общего числа зарегистрированных киберпреступлений.

Структурный анализ совершенных в текущем году мошенничеств свидетельствует о явном преобладании таких способов завладения деньгами потерпевших, как:

Продажа несуществующего товара, на различных Интернет – ресурсах

Очень часто жертвами мошенников становятся пользователи сети Интернет, желающие приобрести различные товары в социальной сети **Instagram - 483 преступления или 43 %**. Продавцы, как правило, просят предоплату за товар, однако такие истории заканчиваются одним - граждане перечисляют предоплату, в дальнейшем связь с продавцом теряется и последние не получают долгожданный товар.

Для примера можно рассмотреть следующие мошеннические учетные записи: @easy_step_by, @original_brand.by, @edelweis.resort, @fox.store.by, @EUROSHINA_BY, @airmac_by, @flowerslovers.by, @_belbet_off, @happysale.by и т.д.

Обман граждан под предлогом вложения средств в криптовалюту, либо сделок с ней на несуществующих биржах и иного заработка в сети Интернет - 135 преступлений или 12 %

Несуществующие инвестиционные проекты и мошеннические биржи - это обманные схемы, в которых инвесторам предлагается вложить

средства в вымышленные или несуществующие бизнес - проекты, или финансовые инструменты с обещаниями высокой прибыли, которая на самом деле не может быть достигнута.

Мошеннические биржи, предлагающие несуществующие инвестиционные проекты, обычно используют различные хитрости и тактики, чтобы привлечь потенциальных инвесторов. Вот несколько типичных характеристик таких мошеннических схем:

•обещания высокой доходности при минимальных рисках: Мошеннические биржи обычно привлекают внимание инвесторов, обещая очень высокие доходы при минимальном или даже отсутствующем риске. Это является привлекательным для людей, желающих получить быструю и легкую прибыль, однако на самом деле такие обещания часто оказываются ложными;

•неясные условия инвестирования и вывода средств: Мошеннические биржи часто предлагают инвесторам неясные и запутанные условия инвестирования и вывода средств. Это может включать в себя скрытые комиссии, высокие пороги для вывода средств или даже отсутствие возможности вывода вложенных денег вовсе;

•использование лживой информации и фальшивых отзывов: Для привлечения новых клиентов мошеннические биржи часто создают ложные отзывы, поддельные рекомендации и искаженные данные о своей деятельности. Это создает иллюзию успешной и надежной компании, призванной убедить инвесторов вложить свои деньги.

Для примера можно рассмотреть следующие мошеннические виды мошеннических проектов:

Пирамиды

Пирамидные схемы являются одними из самых распространенных форм финансового мошенничества. Они предлагают инвесторам «легкую» прибыль за счет привлечения новых участников. Основная идея заключается в том, что старшие участники выигрывают за счет взносов новичков. Такие схемы неустойчивы и, когда приток новых участников замедляется, они обречены на крах, оставляя большинство участников без вложенных средств.

Фейковые криптопроекты

В связи с возросшим интересом к криптовалютам, мошенники также начали использовать криптопространство для своих незаконных целей. Они предлагают ложные криптовалютные проекты с обещаниями быстрой и легкой прибыли. Однако за ними стоят скрытые мотивы и планы, которые могут привести к убыткам для инвесторов.

Звонки мошенников в мессенджерах (Viber, Telegram, WhatsApp) под видом сотрудников правоохранительных органов либо

специалистов банковских и иных учреждений, вынуждающих потерпевших под различными предлогами получать кредиты и переводить денежные средства либо сбережения на подконтрольные злоумышленниками счета - 517 или 46 %

В текущем году наиболее актуальная схема - побуждение открыть кредит. Злоумышленники сообщают жертве о том, что якобы кто - то посторонний пытается открыть кредит на ее имя, поэтому для деактивации таких действий необходимо самостоятельно обратиться в банк и открыть кредит, и в дальнейшем перевести денежные средства на сберегательные счета. Как правило после перевода денежных средств связь с злоумышленников прекращается.

Схема кибермошенничества от имени «Белпочты»

Схема довольно проста - злоумышленники присылают потенциальной жертве сообщение через интернет - мессенджер. В нем сообщают о необходимости уточнения адреса доставки почтового отправления и предлагают перейти по ссылке в Интернете. Невнимательный человек, не проверив адрес, по которому ему предлагают перейти, попадает на фейковый сайт, стилизованный под официальный сайт «Белпочты». Там клиента просят ввести свой адрес, якобы для доставки некоего почтового отправления, и оплатить тариф за услугу «Белпочты» прямо на этой странице, введя реквизиты банковской карты.

Схема кибермошенничества от имени операторов сотовой связи УП «А1» и СООО «МобильныеТелеСистемы»

Злоумышленники пользуются доверием клиентов компании и звонят через мессенджер (WhatsApp, Viber, иной мессенджер), представляются сотрудниками А1. Под предлогом необходимости обновления приложения компании, продления договора оформления сим-карты убеждают установить или переустановить мобильное приложение «Мой А1» и «Мой МТС» на ОС Android не из официального магазина приложения, а из специального установочного АРК-файла, который присылают личным сообщением в мессенджер.

Все действия злоумышленники требуют выполнять строго по их алгоритму. В случае, если вы выполнили указанные действия и установили (или обновили) уже вредоносное приложение, смартфон становиться подконтрольным злоумышленнику. Он получает полный доступ к вашему мобильному телефону, потому что приложение, которое вы установили (обновили)_является фейковым (логотип и содержание точно такое же, как и у оригинального). Смартфон становиться подконтрольным злоумышленнику, после чего у него появляется доступ к данным пользователя, которые хранятся на смартфоне (SMS, личная переписка в мессенджерах и соцсетях, информация о банковских картах и паролях и

т.д.). Таким образом, злоумышленник может устанавливать сторонние приложения, оформлять банковские и иные сервисы и услуги.

Если вы через какой-либо мессенджер (в частности, через Viber) с незнакомого номера получили звонок якобы от имени службы поддержки А1 и МТС, то следует проигнорировать вызов и не перезванивать на номер.

Входящие вызовы в мессенджерах могут быть визуально схожи с обычными звонками с городского или мобильного номера, поэтому стоит быть особенно бдительными и обращать внимание на номера, а также на то, через какой канал осуществляется звонок. Как правило, злоумышленники пытаются заполучить конфиденциальную информацию, а также подталкивают жертв к различным действиям со счетами.

Схема кибермошенничества «Fake BOSS»

С начала года фиксируются неединичные случаи попыток компрометации реквизитов доступа к учетным записям интернет-мессенджеров (Telegram, WhatsApp и др.), зарегистрированным на номера телефонов работников государственных учреждений и организаций.

Свидетельством попыток компрометации послужили поступившие от администрации интернет-ресурса многочисленные сообщения с кодами, которые могут быть использованы злоумышленниками для осуществления несанкционированного доступа к аккаунту, установки «десктопной» версии мессенджера (для персонального компьютера) с целью мониторинга передаваемых сообщений, выгрузки архива сообщений и иных действий.

Злоумышленники осуществляют рассылку сообщений с указанием того, что в скором времени гражданину позвонит или напишет сотрудник вышестоящей инстанции (Министерства образования, МВД, КГБ, КГК, СК, ОВД). Как правило, пугаясь, граждане говорят любую информацию, которую требует сотрудник. Далее просят установить удаленное программное обеспечение, позволяющее получить ему доступ к устройству, либо вести видеозапись с демонстрацией экрана мобильного телефона.

Одновременно зафиксированы случаи массовой рассылки неизвестными отправителями ссылок в интернет-мессенджерах (Telegram, WhatsApp и др.). Побудительным мотивом для перехода по ссылке в сообщениях выступают различные предлоги (просмотр видео, необходимость обновления программ, устранение уязвимостей и другие).

Целью является получение критически важных данных (закрытой служебной информации, реквизитов учетных записей, паспортных данных и иных сведений). Также переход по ссылке может привести к переходу на фишинговый (поддельный) интернет - ресурс заражению вредоносным программным обеспечением, которое позволит злоумышленникам получить удаленный доступ к устройству и контроль над ним.

Наряду с этим в отчетном периоде зарегистрировано **54** вымогательства (ст. 208 Уголовного кодекса), **10** заведомо ложных сообщений об опасности (ст. 340 Уголовного кодекса), **70** фактов незаконного оборота средств платежа и (или) инструментов (ст. 222 Уголовного кодекса), **621** хищение имущества путем модификации компьютерной информации (ст. 212 Уголовного кодекса) и **76** преступлений против компьютерной безопасности (Глава 31 Уголовного кодекса).

Основными способами совершения хищений имущества путем модификации компьютерной информации (ст. 212 Уголовного кодекса), являются **также звонки мошенников в мессенджерах под видом сотрудников правоохранительных органов либо специалистов банковских и иных учреждений, в ходе которых злоумышленники получают доступ к банковским реквизитам граждан (56,4 %).**

Такой способ называется «Вишинг» - это один из методов мошенничества с использованием социальной инженерии (социальная инженерия - это совокупность способов психологического воздействия на поведение человека с целью получения выгоды), который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определенную роль, под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию, или побуждают, убеждают вероятную жертву к совершению определенных действий со своей банковской платежной картой

Он заключается в том, что злоумышленники, используя телефонную связь и, выдавая себя за сотрудников банка или правоохранительных органов, под различными предлогами вводят в заблуждение потерпевших, выясняя сведения о наличии банковских платежных карточках, их реквизитах, паспортных данных с целью последующего хищения денежных средств.

В большинстве случаев при совершении звонков мошенники используют интернет - телефонию, которая позволяет маскировать телефонные номера под номера белорусских операторов связи.

При этом всем известные мессенджеры Viber, Telegram и WhatsApp имеют возможность использования виртуальных номеров.

К примеру, злоумышленники звонят жертве от имени банковского работника и сообщают, что необходимо осуществить какие - либо действия с банковской платежной карточкой, так как кто-то либо пытается похитить с нее денежные средства, либо оформляет кредит, либо проводит подозрительную оплату.

Для большей достоверности в качестве имени пользователя они указывают официальный номер банка либо его название, а для «аватарки» используют логотип или эмблему банковского учреждения.

При этом зачастую они уже владеют минимальной информацией о лицах, которым звонят (имя, отчество, дата рождения, последние цифры банковской карты и др.), что способствует повышению доверия к звонящему и производит на него определенное впечатление.

В дальнейшем преступник просит сообщить информацию о банковской карте - номер, срок действия, трехзначный код на ее обороте, содержание СМС - сообщения, которое в ходе разговора поступает на мобильный телефон, либо устанавливает мобильное приложение, позволяющее злоумышленнику получить удаленный доступ к мобильному телефону, в котором сегодня фактически у каждого имеется интернет - банкинг и, соответственно, доступ к банковскому счету.

Использование фишинговых Интернет - ресурсов (25,4 %)

Фишинг - вид мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей - логинам, паролям, данным лицевых счетов и банковских карт с использованием поддельных интернет - ресурсов, контролируемых злоумышленниками, внешне схожих с настоящими (например, поддельные страницы услуги «Интернет - банкинг» различных банков).

Также в социальных сетях появилась реклама, обещающая «призы от Белагропромбанка». Переходя по ссылке, жертва попадает на поддельную банковскую страницу, на которой мошенники выманивают номера телефонов и иные личные данные, что дает им полный доступ к счетам обманутых и даже возможность оформления онлайн-кредитов.

Основные способы совершения вымогательств (ст. 208 Уголовного кодекса) можно разделить на три основные категории:

•связаны с угрозой распространения личной информации потерпевших, которые последние желали сохранить в тайне **(27 или 50 %)**, как правило фотографий и видеозаписей интимного характера, которые, в большинстве случаев, потерпевшие самостоятельно пересылали злоумышленникам, полагая, что общаются с потенциальным партнером противоположного пола для знакомства.

•связаны с блокированием компьютерной информации физических лиц **(24 или 44,4%)**. При этом в подавляющем большинстве случаев отмечается блокирование учетных записей Apple ID посредством ввода авторизационных данных, предоставленных злоумышленниками под благовидными предлогами, что в последующем не позволяет потерпевшим полноценно использовать свои мобильные устройства.

•связаны с угрозой применения насилия **(3 или 5,6 %)**.

Стоит отметить, что **81%** всех совершенных заведомо ложных сообщений об опасности с использованием сети Интернет, составляют **«сватерскую»** направленность, то есть отправку заведомо ложного сообщения об опасности от лица жертвы, посредством электронной почты.

Преступления против компьютерной безопасности (Глава 31 Уголовного кодекса) в большинстве случаев возбуждаются по фактам неправомерного завладения учетными записями мессенджеров и социальных сетей, таких как (Telegram (34), WhatsApp (3), Instagram (7), Facebook (1) и «ВКонтакте» (13).

Основными факторами, способствующими совершению киберпреступлений, являются халатность, излишняя доверчивость граждан, мнимая возможность быстрого обогащения, получение крупных сумм денежных средств, а также недостаточное информирование населения о способах и методах применяемыми преступниками при совершении указанных преступлений.

Знание основных схем и способов обмана позволяет гражданам быть более внимательным и осторожным, что, в свою очередь, помогает предотвратить случаи совершения киберпреступлений.

Чтобы не стать жертвой киберпреступников, необходимо хотя бы минимально следовать следующим правилам:

Телефонное мошенничество

•Вам звонят в мессенджере из Национального банка;

•чтобы спасти Ваши деньги, надо перевести их на безопасный счет;

•это КГБ, милиция, следственный комитет и т.д., Вы должны помочь нам в расследовании;

•назовите номер банковской карты, дайте код их СМС, сообщите номер паспорта;

•Ваша карта заблокирована;

•Ваш родственник попал в беду;

•Вам нужно установить приложение на свой мобильный телефон.

Если вы слышите любую из этих фраз по телефону, знайте - это мошенники!!! **Что здесь общего?**

•к Вам обращается значимое лицо;

•Вас пугают потеряй денежных средств, уголовным преследованием, проблемами у близких;

•у Вас запрашиваю персональные данные;

•Вам не дают времени подумать.

Рекомендации:

•немедленно прекратите разговор;

•самостоятельно перепроверьте информацию, позвоните в банк, милицию, родственнику и т.д.;

•**не сообщайте по телефону:** паспортные данные, реквизиты банковской карты; реквизиты доступа к Интернет и мобильному банку; поступающие на мобильный телефон СМС сообщения;

•не устанавливайте по указанию звонившего никаких приложений на свой телефон.

Помните!!! Сотрудники государственных органов не звонят в мессенджерах (Viber, Telegram, WhatsApp и т.д.) и - с зарубежных номеров.

Мошенничество на сайтах объявлений и в социальных сетях

Мошенники, выдавая себя за представителей известных торговых компаний, размещают объявления на торговых площадках и в социальных сетях по продаже несуществующих товаров, предоставлении различного рода услуг, аренды недвижимости и т.д.

Как правило мошенники:

•для общения с клиентами используют только мессенджеры, от личного или голосового общения по мобильному телефону воздерживаются;

•на порядок занижают цены на продаваемый товар;

•требуют перевода на банковскую карту предоплаты или полной стоимости товара;

Рекомендации:

•тщательно проверяйте информацию о продавце;

• совершайте покупки на официальных маркетплейсах;

•не оплачивайте товар до его получения.

Мошеннические приложения

Данный способ мошенничества заключается в том, что жертве, в мессенджере, либо с зарубежного абонентского номера, на мобильный телефон поступает телефонный звонок от оператора сотовой связи, в ходе которого оператор уведомляет, что компания переходит на новое мобильное приложение и следует его переустановить, после чего, посредством мессенджеров предоставляет ссылку на его загрузку. На самом деле приложение выполняет функции удаленного доступа к телефону и позволяет злоумышленникам получать изображение с экрана с целью завладения кодами в поступающих смс-сообщениях (устанавливается, как дополнительное приложение к основному и имеет иконку соответствующего оператора сотовой связи)

Рекомендации:

•отключить доступ в Интернет;

•удалить приложение;

•при наличии поступающих сообщений из банковских учреждений, заблокировать карт-счета.

Мошеннические биржи

Мошеннические биржи, предлагающие несуществующие инвестиционные проекты, обычно используют различные хитрости и тактики, чтобы привлечь потенциальных инвесторов. Вот несколько типичных характеристик таких мошеннических схем:

•обещания высокой доходности при минимальных рисках (мошеннические биржи обычно привлекают внимание инвесторов, обещая очень высокие доходы при минимальном или даже отсутствующем риске, что является привлекательным для людей, желающих получить быструю и легкую прибыль, однако на самом деле такие обещания часто оказываются ложными;

•неясные условия инвестирования и вывода средств: Мошеннические биржи часто предлагают инвесторам неясные и запутанные условия инвестирования и вывода средств (это может включать в себя скрытые комиссии, высокие пороги для вывода средств или даже отсутствие возможности вывода вложенных денег вовсе;

•использование лживой информации и фальшивых отзывов инвесторов вложить свои деньги.

Рекомендации:

Для того чтобы не стать жертвой мошеннических схем с несуществующими проектами, необходимо принимать тщательные меры по защите своих финансов:

•тщательно проверяйте информацию о компании;

•остерегайтесь аномально высокой доходности (будьте бдительны, если какой-то проект обещает нереально высокую доходность без рисков);

•не торопитесь с принятием решений, не поддавайтесь на давление временем и не принимайте поспешных решений, хорошо изучите каждое инвестиционное предложение, обратив внимание на все детали и условия;

•консультируйтесь с финансовыми экспертами;

•используйте проверенные инвестиционные платформы (при выборе площадки для инвестиций отдавайте предпочтение проверенным биржам или инвестиционным компаниям, у которых есть хорошая репутация на рынке).