В настоящее время сеть Интернет и компьютерные технологии стремительно проникают во все сферы жизнедеятельности человека. С одной стороны, это открывает перед обществом ряд перспектив, с другой - влечет появление новых рисков и угроз. Бурное развитие телекоммуникационных технологий, развитие дистанционных способов совершения преступлений, а также недостаточно высокий уровень цифровой безопасности граждан привели к увеличению количества киберпреступлений.

Вопросы цифровой трансформации преступности сегодня являются одними из наиболее злободневных. И от того, насколько эффективно удастся противостоять этому вызову, зависит не только защищенность прав и интересов граждан, но и информационная безопасность общества и государства. При этом универсальных подходов, позволяющих эффективно противодействовать высокотехнологичным преступлениям, не выработано ни одним государством мира.

*Пример 1. В результате проведения оперативно-розыскных мероприятий установлены и задержаны участники преступной группы под названием «A** D******Y», специализирующихся на хищениях денежных средств пользователей торговой площадки «k***r.by» (Справочно: Согласно имеющимся сведениям указанной преступной группы за период времени с 29.07.2021 по 04.09.2022 совершили более 5 000 эпизодов хищений денежных средств на общую сумму не менее 1 500 000 белорусских рублей).*

Наиболее актуальные виды киберпреступлений

Одним из самых распространенных киберпреступлений традиционно остается хищение денежных средств путём модификации компьютерной информации. Причем в большинстве случаев эти преступления становятся возможны из-за беспечности самих потерпевших, предоставивших реквизиты доступа к своим банковским счетам.

Преступники завладевают реквизитами, необходимыми для осуществления преступных транзакций, посредством следующих основных способов:

Вишинг «звонок из банка», «звонок от имени сотрудника правоохранительного органа», «звонок от имени сотрудника сотовой компании», звонок от имени руководителя учреждений здравоохранения или учебного заведения»

Вишинг (англ. vishing, от voice phishing) - один из методов мошенничества с использованием социальной инженерии, который заключается в выведении злоумышленников жертвы на желаемую модель поведения с целью завладения конфиденциальной информации для последующего хищения средств.

Как правило, для совершения звонка преступники используют один из распространенных мессенджеров, используя, в том числе, функцию подмены номера. Как следствие, у потерпевшего на экране мобильного телефона может отображаться совершенно любой номер телефона, заданный злоумышленником. Также преступники маскируются под логотипом узнаваемых белорусских банков, вводя в заблуждение потенциальных жертв.

От имени банковского сотрудника или представителя правоохранительных органов злоумышленники сообщают жертве, что необходимо осуществить какие-либо действия с банковской платежной картой, так как кто-то либо пытается похитить с нее денежные средства, либо оформляет кредит, либо производит подозрительную оплату. Завладев реквизитами банковской платежной 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.

Пример 1. В середине марта 2024 года уроженке г. Могилева, работающей на одном из предприятий города, посредством мессенджера «WhatsApp» позвонило неизвестное лицо. Звонивший представился сотрудником компании «А-1», под предлогом продления договора на оказание услуг убедил потерпевшую установить якобы оригинальное приложение «Мой А-1.apk», на самом деле являющееся программой удаленного доступа, предоставляющей полный доступ, включая камеры, к мобильному телефону. После чего путем модификации компьютерной информации совершило с банковских счетов могилевчанки хищение 4 400 рублей НБ Республики Беларусь.

«Фишинг»

Фишинг (от англ. fishing - рыбная ловля, выуживание) — один из видов мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (логинам и паролям) и последующего хищения денежных средств.

Наиболее часто данная преступная схема реализовывает в отношении клиентов торговых интернет-площадок. Выступая в роли покупателя, злоумышленник находит продавца товара и вступает с ним в переписку в мессенджерах *(«Viber», «Telegram», «WhatsApp»)*. Он сообщает, что товар его заинтересовал и уже якобы совершил предоплату (зачастую высылается скриншот электронного чека о перечислении средств). Для того, чтобы получить данные средства, продавцу якобы необходимо пройти по гиперссылке и ввести данные.

Невнимательный интернет-пользователь может и не заметить подмены, так как подобные страницы визуально схожи с оформлением сайтов известных сервисов *(Куфар, ЕРИП, CDEK, Белпочта, сайты различных банков и др.)*. Адрес поддельной веб-страницы также может напоминать реальный (kufar- dostavka.by, erip-online.com, belarusbank24.xyz, cdek-zakaz.info и др.).

Если жертва «попадется на удочку» и заполнит форму, соответствующие реквизиты доступа к банковскому счету окажутся у преступника. Через считанные минуты злоумышленник осуществляет доступ к банковскому счету и переводит денежные средства на контролируемые им банковские счета или электронные кошельки, зарегистрированные на подставных лиц.

Пример 1. Жительница г. Могилева на торговой Интернет-площадке разместила объявление о продаже комбинезона. Вскоре в мессенджере «Viber» ей поступило сообщение от неизвестного абонента, который сообщил о желании приобрести товар. Затем он прислал ссылку «https://evropochta.by-prodazha.com», пояснив, что женщине необходимо ввести реквизиты своей банковской платежной карты для последующего перевода денег за комбинезон. Она прошла по ссылке, ввела требуемую информацию, и вскоре с ее счета преступник похитил 560 рублей.

В последнее время участились случаи создания фишинговых сайтов, ориентированных под запросы пользователей в поисковых системах. Граждане попадают на них прямо из поисковых систем «Google» и «Yandex» после запросов типа «Беларусбанк личный кабинет», «Белагропромбанк интернет банкинг» и т.д. Увидев знакомый заголовок и логотип сайта в выдаче результатов поиска и не удостоверившись в соответствии адреса сайта действительному доменному имени банковского учреждения, потерпевший заполняет открывшуюся форму авторизации. В результате введенные данные отправляются преступнику, а не банку.

Пример 2. Злоумышленник создал поддельный сайт СДБО Интернет-банкинга ОАО «Белагропромбанк». 20.02.2024 могилевчанка, при помощи рабочего персонального компьютера посетила глобальную компьютерную сеть Интернет при помощи Интернет-браузера «Google Chrome», с целью дальнейшего посещения сайта СДБО Интернет-банкинга ОАО

«Белагропромбанк» для проверки текущего баланса на банковском счете. Заявительница ввела в поисковую строку запрос «Белагропромбанк Интернет-банкинг вход», после чего перешла по первой индексируемой поисковой системой «Google» ссылке, ввела свои личные данные для входа в личный кабинет СДБО Интернет-банкинга ОАО «Белагропромбанк», после чего ввела сеансовый ключ, пришедший ей на мобильное устройство в виде SMS-оповещения. На экране персонального компьютера появилась загрузка. Однако, спустя некоторое время на мобильный телефон заявительницы поступило SMS-оповещение о списании с банковского счета денежных средств в размере 1200 рублей.

Иные способы совершения киберпреступлений

Свободный доступ к банковской карте

В ряде случаев причиной хищений с банковских счетов становятся не хитрые схемы мошенников, а банальная утеря карты, оставление ее в легкодоступном месте или передача иным лицам для осуществления разовых платежей. Разновидностью подобного легкомыслия является хранение фотоизображений банковских карт или платежных реквизитов в памяти мобильного телефона, в почтовом аккаунте или дистанционном облачном хранилище. При несанкционированном доступе к такому хранилищу преступник получает беспрепятственный доступ к банковскому счету его владельца.

Риск остаться без заработанных денежных средств также увеличивает хранение PIN-кода рядом с картой (например, записанным на бумажке в кошельке или на самой банковской карте).

Покупка с предоплатой

Наиболее простой, но от этого не менее работающей формой интернет-мошенничества, является размещение преступниками объявлений о продаже каких-либо товаров по бросовым ценам. Но для его получения (якобы посредством почтовой пересылки или службы доставки) требуется перечисление предоплаты или задатка на указанные «продавцом» банковскую карту, электронный кошелек. Обычно после перечисления ожидаемый товар так и не поступает, а «продавец» перестает выходить на связь.

В последнее время наиболее распространенным видом мошенничества стали продажи «сезонных» товаров, т.е. в зимний период это шубы, елки, в весенне-летний период это качели и другой

садовый инвентарь, а также элементы одежды. Наиболее часто объявления размещаются в социальной сети «Инстаграмм».

Шантаж

В некоторых случаях злоумышленники могут угрожать разглашением различных компрометирующих сведений с целью вымогательства.

Социальные сети - это кладезь персональной информации о человеке. Получив несанкционированный доступ к страницам в социальных сетях, переписке электронных почтовых ящиков и облачным аккаунтам и завладев изображениями, не предназначенными для публичного просмотра, преступники вступают в переписку с потерпевшими, требуя разные денежные суммы и угрожая в случае отказа распространить их в сети Интернет.

Звонок от имени руководителя

В последнее время участились случаи поступления звонков (сообщений) сотрудникам тех либо иных учреждений якобы от имени руководителя, в ходе общения с которым потенциальной жертве преподносят мнимую (вымышленную) ситуацию о негативных действиях коллег по работе. Пример: *учителю начальных классов Петровой А.А. одной из школ в г. Могилева поступил звонок в мессенджере «Telegram», от пользователя, который был подписан Иванов В.В. В свою очередь, Иванов В.В. является директором школы, в которой работает Петрова А.А., однако контакта директора в мобильном телефоне Петрова А.А. не имеет. В ходе общения, Иванов В.В. начинает пояснять, что с ним связались сотрудники КГБ Республики Беларусь, которые проводят закрытую проверку в отношении одного из работников школы, который был уличен в совершении противоправных действий. Для того, чтобы Петрова А.А. не стала соучастником противоправного деяния, Иванов В.В. перенаправляет ее на общение с сотрудником КГБ, который, в свою очередь, под предлогом оказания помощи, а также проведения тех либо иных процессуальных действий, убеждает Петрову А.А. предоставить доступ к своему мобильному телефону посредством установления приложения удаленного доступа, после чего похищает денежные средства, находящиеся на расчетных счетах, либо же просит задекларировать (подтвердить) законность имеющихся на руках наличных денежных средств под предлогом перевода на безопасный счет.* В случае поступления таких звонков либо же сообщений, необходимо вживую связываться с руководителем, либо же иным сотрудником, от

имени которого оно поступило. Ни в коем случая нельзя общаться с виртуальным пользователем в одиночку.

Основные правила цифровой гигиены

Никогда, никому и ни при каких обстоятельствах не сообщайте реквизиты своих банковских счетов и банковских карт, в том числе лицам, представившимся сотрудниками банка или правоохранительных органов.

Также не следует сообщать в телефонных разговорах и при общении в соцсетях полный номер карточки, срок ее действия, код CVC/CVV (находящиеся на обратной стороне карты), логин и пароль к интернет-банкингу, паспортные данные, кодовое слово (цифровой код) из SMS-сообщений.

В случае поступления звонка «от сотрудника банка» необходимо уточнить его фамилию, номер телефона, после чего завершить разговор и самим позвонить в банк или в круглосуточную службу сервиса, номер которой написан на оборотной стороне платежной карты. Сообщите о случившемся. Скорее всего, никаких несанкционированных операций не было, и никто из банка не звонил.

В том случае, если с использованием Вашего счета и правда кто-то будет пытаться совершить несанкционированные операции и банк это заметит, то его сотрудники сперва инициативно заблокируют банковскую платежную карту, затем сообщат Вам причину принятого решения (ничего не уточняя) и пригласят посетить банк с паспортом для получения наличных денежных средств и написания заявления на перевыпуск карты.

Учтите: сотрудники банков никогда не используют для связи с клиентами мессенджеры («Viber», «Telegram», «WhatsApp»).

В настоящее время просто необходимо наличие второй банковской платежной карты, не привязанной к основному банковскому счету (например, зарплатному).

Этой картой рассчитывайтесь в сети Интернет, заранее пополняя ее на необходимую сумму. В таком случае Вы сможете обезопасить свой основной банковский счет.

Многие банки предлагают своим клиентам услугу выпуска «виртуальной карты». Процесс ее открытия не требует посещения клиентом банка и представляет собой достаточно быстрый процесс. В итоге Вы станете обладателем электронного аналога банковской карты, посредством которой сможете рассчитываться за услуги в сети Интернет без риска скомпрометировать основной банковский счет. Просто перед оплатой пополните ее необходимой суммой с основной карты - и никаких проблем!

Ни в коем случае не предоставляйте доступ к мобильному устройству посторонним лицам!

Никогда не устанавливайте по просьбам незнакомых лиц программы удаленного доступа, такие, например, как «AnyDesk», «RustDesk» и др. Не сообщайте незнакомым лицам сеансовые коды! Через эти приложения мошенники могут получить доступ к мобильному приложению интернет - банкинга на Вашем устройстве и совершить хищение денежных средств.

Каждый владелец банковских платежных карт может настроить собственный алгоритм безопасности при их использовании.

Для обеспечения сохранности денежных средств, размещенных на банковских счетах, каждый держатель карточки посредством систем дистанционного банковского обслуживания может установить индивидуальные ограничения (лимиты/запреты).

Среди основных - следующие:

- подключение технологии 3D-Secure (обязательное подтверждение операций, совершаемых держателями карточек с применением их реквизитов в сети Интернет);
- установление банком-эмитентом ограничение на проведение расходных операций (максимальная сумма и количество операций в определенный период времени);
- возможность самостоятельно устанавливать ограничения (на проведение операций в сети Интернет, на совершение операций в конкретной стране, на совершение отдельных видов операций).

Для доступа к системам дистанционного банковского обслуживания и личным аккаунтам необходимо использовать сложные пароли, исключающие возможность их подбора.

Рекомендуется составлять комбинации паролей не менее чем из 12 знаков *(цифры, буквы и символы в разном регистре)*. Создавайте уникальные пароли для каждого сервиса в отдельности. Стоит воздержаться от паролей, составленных из дат рождения, имен, фамилий - то есть тех, которые легко вычислить из общедоступных источников информации *(например, тех же социальных сетей)*. Также следует регулярно менять пароли, чем чаще - тем лучше. Пользуйтесь только проверенным менеджерам паролей!

При поступлении в социальных сетях сообщений от лиц, состоящих в категории «друзья», с просьбами о предоставлении денежных средств в долг или с просьбой пройти по ссылке и проголосовать - не следует сразу же отвечать на подобные сообщения!

Нередко такие просьбы рассылаются от имени друзей преступниками, взломавшими аккаунт в социальной сети и получившими доступ к конфиденциальной переписке. Поэтому сначала необходимо связаться с этим человеком (по телефону, лично встретиться) и уточнить, действительно ли он нуждается в помощи.

В целях защиты устройств необходимо использовать лицензионное программное обеспечение, регулярно обновлять программное обеспечение и операционную систему.

Установить антивирусную программу следует не только на персональный компьютер, но и на смартфон, планшет и регулярно обновлять ее.

Обязательно расскажите об этих основных правилах «цифровой гигиены» своим родственникам, близким, знакомым и друзьям, ведь в силу возраста или недостаточного уровня финансовой грамотности они могут быть особенно уязвимы для действий киберпреступников!

В Ленинском РУВД г.Могилева с начала 2024 года зарегистрировано 62 преступлений, ответственность за совершение которых предусмотрена ст.222 УК Республики Беларусь. В основном указанные преступления были совершены лицами в возрасте от 16 до 24 лет, в том числе и те, которые имеют постоянную работу, однако по какой-либо причине денежных средств указанным гражданам не хватало, в связи с чем они находили объявление в сети «Интернет» (*чаще мессенджер Telegram*) о подработке. Подработка заключалась в том, что гражданину необходимо было предоставить доступ к личному кабинету «Интернет-банкинга» третьему лицу, который вел переписку в мессенджере «Telegram». Вся процедура происходила в основном в режиме «онлайн». Жители г.Могилева открывали на свое имя счета в различных банковских учреждениях, наиболее популярными являются: ОАО «БНБ-Банк», ОАО «Сбер Банк». После чего при создании личного кабинета необходимо было придумать логин и пароль, который в последующем передавался третьим лицам зачастую за денежное вознаграждение. Деньги жители г.Могилева получали на свои зарплатные карты. Таким образом в действиях граждан, которые предоставляли реквизиты доступа к личному кабинету «Интернет-банкинга» образовывался состав преступления, предусмотренный ст.222 УК Республики Беларусь. **Счета, передаваемые третьим лицам, в основном использовались в мошеннических операциях**.

«Незаконный оборот средств платежа и (или) инструментов». Ответственность за совершение указанного деяния.

Уголовный Кодекс Республики Беларусь
Статья 222. Незаконный оборот средств платежа и (или) инструментов

1. Изготовление в целях сбыта либо сбыт поддельных банковских платежных карточек, иных платежных инструментов и средств платежа, а равно совершенное из корыстных побуждений незаконное

распространение реквизитов банковских платежных карточек либо аутентификационных данных, посредством которых возможно получение доступа к счетам либо электронным кошелькам, –наказываются штрафом, или ограничением свободы на срок от двух до пяти лет, или лишением свободы на срок от двух до шести лет.

2. Те же действия, совершенные повторно, либо организованной группой, либо в особо крупном размере, –наказываются ограничением свободы на срок от трех до пяти лет или лишением свободы на срок от трех до десяти лет со штрафом или без штрафа.

То есть преступлением являются следующие действия:

1. Изготовление поддельных платежных банковских карт (далее БПК), если имелась цель сбыта этих карточек;
2. Сбыт поддельных БПК независимо от возможности или безвозмездности данного действия;
3. Изготовление с целью сбыта иных платежных инструментов и средств платежа (приспособлений с помощью которых можно осуществить платеж);
4. Сбыт поддельных платежных инструментов и средств платежа;
5. Распространение из корыстных побуждений реквизитов БПК (номер, срок действия, код CVV, CVC, CVP и др.), фактическое получение вознаграждения при этом не требуется;
6. Распространение логина и пароля, фактическое получение вознаграждения при этом также не требуется;

Размер штрафа за совершение данного преступления устанавливается уголовным кодексом в пределах от 300 до 5000 базовых величин (12000 — 200 000 бел. рубл.)

Для несовершеннолетних применяется особая норма закона, предусматривающая наложение штрафа в размерах от 5 до 50 базовых величин.