Информационные материалы
о формах и методах совершения
киберпреступлений
в отношении пожилых граждан

За 5 месяцев 2025 года от киберпреступлений, зарегистрированных на территории г. Минска, пострадало более 480 граждан возраста 60 лет и старше, две трети из которых в результате мошеннических действий, одна треть – в результате хищений путем модификации компьютерной информации, (1,2%) – в результате совершения преступлений против информационной безопасности. Среди указанной категории граждан чаще от киберпреступлений претерпевали женщины (74,2%).

Анализ уголовных дел по видам преступлений показал, что жертвами хищений путем модификации компьютерной информации стали 163 гражданина пожилого возраста, из них 22 лица пострадало от таких хищений, совершенных в крупном и особо крупном размерах (сумма похищенных денежных средств составляет не менее 10 500 белорусских рублей). В 121 случае интернет-хищений (из 163) жертвами стали женщины(из них 17 совершены в крупном и особо крупном размере), в остальных 42 – мужчины (в 5 случаях совершены в крупном и особо крупном размере).

Жертвами мошеннических действий, совершаемых с использованием информационно-коммуникационных технологий, стали 311 человек в возрасте 60 лет и старше, преобладающее большинство из которых женщины (74,3%). От мошеннических действий, совершенных в особо крупном и крупном размере, пострадало 147 человек указанного возраста, из них женщины (70,7%).

Наряду с этим, 6 пожилых граждан (64-73 года) стали жертвами преступлений против компьютерной безопасности (Глава 31 УК).

Мониторингом способов совершения хищений путем модификации компьютерной информации установлено, что две трети из них совершены путем вишинга (117 из 163 или 71,8%), когда потерпевшим поступали звонки посредством мессенджеров (Telegram, Viber, WhatsApp) от псевдосотрудников правоохранительных органов, банковских учреждений, сотовых компаний, работников коммунальных предприятий. Каждый девятый пожилой человек (18 из 163 или 11,0%) пострадал от перехода по фишинговым ссылкам под предлогом оплаты доставки товаров в интернете. Практически каждое восьмое хищение путем модификации компьютерной информации (21 из 163 или 12,9%) связано с физическим доступом к банковским платежным картам (далее – БПК) либо к системе дистанционного банковского обслуживания потерпевших

(похищенные, утерянные, добровольно переданные БПК либо использование мобильного телефона жертвы).

Две трети мошеннических действий, совершенных в отношении пожилых граждан, связаны с вишингом (205 из 311 или 65,9%). Почти каждый шестой такой гражданин (55 из 311 или 17,7%) потерял денежные средства под предлогом их вложения в криптовалюту либо сделок с ней на фиктивных биржах и иного заработка в сети Интернет.

В 40 случаях (12,9%) граждане возраста 60 лет и старше стали жертвами аферистов под предлогом приобретения несуществующих товаров (услуг) на интернет-ресурсах (различные торговые интернет-площадки). Еще у 2 потерпевших взломали учетные записи (аккаунты) в соцсетях и мессенджерах (ОК, Telegram, Instagram, WhatsApp и пр.) с последующей рассылкой сообщений от их имени с просьбой одалживания денег либо оказания материальной помощи в связи с трудной жизненной ситуацией. Кроме того, под видом руководителя организации (fake boss), требующего оказать содействие правоохранительным органам в проверке на предмет причастности к финансированию террористической деятельности либо под предлогом одалживания денежных средств, пострадало 3 работающих пенсионера. Жертвами знакомств в интернет-пространстве стали 5 женщин и 1 мужчина возраста 60 лет и старше.

Исходя из проведенного анализа следует, что основная доля киберпреступлений, от которых пострадали пожилые граждане, совершена путем вишинга (322 потерпевших из 481 или 66,9%), т.е., как указывалось выше, посредством звонков от имени сотрудников (работников, представителей) правоохранительных органов, банковских учреждений, сотовых компаний, работников коммунальных (Энергосбыт, Водоканал, Мингаз и т.п.) и телекоммуникационных предприятий (Белтелеком). Главной причиной тому являются психологические особенности потерпевших, в частности склонность к безрассудному доверию неизвестным лицам. Кроме того, злоумышленники используют различные психологические приемы и методы запугивания и убеждения, в результате которых без вмешательства посторонних граждан жертва, как правило, в приоритетном порядке выполняет активные продолжительные действия, направленные на получение и перевод денежных средств в интересах неустановленного лица.

В связи с изложенным при проведении профилактической (разъяснительной) работы с пожилыми гражданами необходимо акцентировать внимание последних именно на скептическом отношении, излишней доверчивости и развитии критического мышления к различного рода звонкам, поступающим им как посредством мобильной связи, так и посредством городских телефонных линий, под видом сотрудников

правоохранительных органов, Национального банка Республики Беларусь и иных банковских учреждений, представителей операторов сотовых компаний, работников «Энергосбыта», «Водоканала», «Мингаза», «Белтелекома» и т.п.

Опишем мошенническую схему, связанную со звонками по стационарной связи.

Злоумышленник в разговоре сообщает о необходимости дистанционного продления (перезаключения) договора на оказание услуг, замены устаревшего оборудования, оперативной сверки показателей счетчиков и пр. При этом для верификации и удобства требует предоставить персональные данные (идентификационный номер паспорта, номер мобильного телефона, иные личные данные). Параллельно, уже на мобильный телефон жертвы (как правило посредством Viber), поступает звонок от сотрудника правоохранительных органов или банка, который сообщает, что в данный момент по стационарному телефону жертва общается с мошенниками и что разговор необходимо прервать. После этого, «псевдоправоохранитель» действует по стандартной мошеннической схеме и сообщает, что:

1) на имя потерпевшего оформили кредиты;

2) с расчетный счетов потерпевшего осуществляется финансирование террористической деятельности либо военных действий в Украине;

3) необходимо оказать помощь правоохранительным органам в поимке аферистов;

4) в связи с тем, что в отношении потерпевшего возбуждено уголовное дело и у него в ближайшее время по месту жительства будет проведен обыск, необходимо срочно обезопасить накопленные сбережения, для чего осуществить их декларирование либо перевод на специальный (безопасный) счет;

5) оказать содействие другим жертвам мошенников, которые в силу преклонного возраста или физических особенностей не могут самостоятельно обратиться в банк для зачисления наличных денежных сбережений на безопасный счет.

После всего услышанного, жертва испытывает эмоциональный шок. Ведь сложно поверить, что это все четко спланированная мошенническая схема. Потерпевшие идя на поводу аферистов следуют их инструкциям и добросовестно исполняют все, что те от них требуют, даже продают собственное жилье и вырученные деньги также переводят на предоставленные злоумышленниками счета.

Необходимо отметить, что мошенники до такой степени втираются в доверие жертв, что при попытках ИСТИННЫХ сотрудников милиции

или работников банковских учреждений их образумить, чаще всего игнорируют все разумные доводы.

Приведем пример одного из таких мошенничеств:

В начале мая шестидесятилетнему Николаю Анатольевичу на домашний телефон позвонила женщина, которая представилась сотрудницей «Энергосбыта» и сообщила о необходимости замены счетчиков. Пожилого мужчину данный факт не смутил, так как около 1 месяца назад он оставлял заявку на замену счетчиков.

Сотрудница «Энергосбыта» попросила предоставить идентификационный номер паспорта, для подтверждения заявки. После окончания разговора с указанной сотрудницей Николаю Анатольевичу на мобильный телефон посредством мессенджера «Viber» с белорусского мобильного номера телефона позвонил ранее неизвестный мужчина, который представился капитаном Князевым Виталием Владимировичем из управления Следственного комитета Республики Беларусь и в ходе разговора начал пояснять, что у них сработала специальная система по предупреждению мошеннических звонков с неизвестных номеров. В ходе диалога Князев В.В. пояснил, что пожилой минчанин стал жертвой мошенников, которые по личному номеру паспорта через подставных лиц берут кредиты. Также Князев В.В. пояснил, что с потенциальным потерпевшим должен связаться специалист из Национального Банка Республики Беларусь. После окончания звонка от Князева В.В., посредством мессенджера «Viber» позвонил неизвестный мужчина, который представился как Исаев Игорь Леонидович - специалист Национального Банка, и начал пояснять, что в настоящее время участились случаи мошенничества в Республике Беларусь, а именно после предоставления личных данных происходит взятие кредитов, снятие пенсий под предоставленные данные. В ходе разговора Исаев И.Л. разговаривал очень четко, ссылался на нормативно-правовые акты Республики Беларусь, в связи с чем, каких-либо сомнений у Николая Анатольевича по данному поводу не возникало. В процессе разговора Исаев И.Л. пояснил, что все банковские карточки Николая Анатольевича решением Национального Банка будут заблокированы, и все денежные средства пропадут. Также Исаев указал, что зафиксированы попытки получения кредитов в различных банках столицы. Для того чтобы вычислить мошенников, нужно взять контрольные кредиты, и в последующем сделать перевод по их погашению. Николай Анатольевич снял последние денежные средства, которые у него имелись после чего направился в банковские учреждения где оформил договоры на кредиты. При оформлении указанных кредитов сотрудники банков интересовались для каких целей ему нужны денежные средства и не находится ли он под влиянием третьих лиц, а также предупреждали о мошенниках, на что тот пояснил, что денежные средства нужны на личные нужды.

Получив кредитные средства Николай Анатольевич перевел их на реквизиты банковской карты, которые указал ему Исаев И.Л.

Необходимо отметить, что при осуществлении потерпевшим переводов, представители банков уточняли, куда, кому и с какой целью Николай

Анатольевич переводил деньги, разъясняя ему, что он действует нелогично и скорее всего находится под чьим-то влиянием, то есть мошенников.

Наряду с этим, потерпевшему по мобильной связи звонил участковый инспектор милиции и расспрашивал кому тот делал переводы. Во время разговора с участковым Николай Анатольевич «плавал» и понимал, что все то, что ему описывает НАСТОЯЩИЙ сотрудник милиции в качестве преступной схемы, аналогичным способом происходит и с ним сейчас. В тот момент Николай Анатольевич начал осознавать, что свои кредитные деньги он перевел мошенникам, однако участковму также не сказал правду, обманув его, что распоряжается деньгами по своему усмотрению и попросил впредь его не беспокоить.

Не желая быть обманутым со стороны якобы спецслужб, 60-летний мужчина решил позвонить Исаеву И.Л. и сообщить о своих предположениях об участии в противоправных действиях, однако Исаев И.Л. уверил его, чтобы тот ни от кого не брал трубки, кроме него, Князева В.В., а также Сафронова Кирилла Алексеевича, который в последующем позвонил по видеосвязи и представился начальником Следственного отдела и руководителем Князева. Сафронов разъяснял потерпевшему, что все деньги по кредиту ему вернут. При этом Сафронов был одет в форменное обмундирование, в связи с чем каких-либо сомнений у Николая Анатольевича снова не возникло.

Далее в ходе телефонной беседы Исаев сообщил, что Николаю Анатольевичу нужно будет ехать в Москву, чтобы помочь участию в специальной операции по выявлению мошенников.

Так, по указанию Исаева, с использованием кодового слова, озвученного им же, мужчина забрал крупную сумму денежных средств у двух минчанок (75 и 45 лет), которые последние передали ему в целлофановых пакетах. Далее по указанию Исаева приобрел билет на поезд до Москвы.

По приезду в г. Москва, Николай Анатольевич заселился в гостиницу «Канна» и проживал там на протяжении суток. На следующий день ему позвонил Исаев, который сообщил, что тот должен встретиться с его коллегой. Далее
по прибытию в указанное Исаевым место, к Николаю Анатольевичу подошел молодой человек 28-30 лет в потрепанной одежде, который имел неопрятный внешний вид. Николай Анатольевич передал ему денежные средства, после чего вернулся обратно в гостиницу. По возвращению в гостиницу Исаев, Князев и Сафонов перестали выходить «на связь».

По возвращению в Минск к Николаю Анатольевичу по месту жительства прибыли сотрудники столичной милиции, которые сопроводили его в ближайшее РУВД. И только в РУВД Николай Анатольевич окончательно убедился, что с ним до этого общались мошенники.

При беседе с сотрудниками милиции Николай Анатольевич пояснял, что неоднократно слышал в новостях и телепередачах о преступных схемах мошенников, более того помочь разобраться в ситуации ему пыталась и супруга, но Николай Анатольевич решил игнорировать все ее доводы, полагая, что он сам

знает, как лучше поступить и в итоге стал жертвой аферистов и соучастником преступления.

В текущем году зафиксировано несколько случаев совершения мошеннических действий под предлогом прохождения медицинской диспансеризации. Схема идентична мошенничествам, совершенным лжеработниками «Энергосбыта», «Водоканала», «Мингаза», «Белтелкома». Основная цель аферистов при таких звонках – заполучить персональные данные гражданина.

Пример:

В середине мая пенсионерке посредством городской электросвязи поступил звонок от «сотрудника местной поликлиники», который пригласил ее на диспансеризацию. Для составления заявки на прохождение указанной процедуры (оформления предварительной записи, талона) минчанка продиктовала звонившему мобильный номер телефона и идентификационный номер паспорта.

В последующем пенсионерке посредством мессенджеров Viber и Telegram стали поступать звонки от неизвестных лиц, которые представлялись сотрудниками Следственного комитета и Национального банка Республики Беларусь. Данные лица сообщили, что на банковские счета, эмитированные на ее имя, мошенники переводят крупные денежные суммы, в связи с чем по месту жительства последней будет проведен обыск. Если при обыске будут обнаружены незадекларированные денежные средства они будут изъяты.

Пенсионерка собрала все хранившееся дома сбережения и при помощи банковского терминала перевела их на обозначенный мошенниками счет.

Нередки случаи, когда после установки программы удаленного доступа злоумышленник оформляет онлайн-кредит на имя потерпевшего без его ведома. Название приложения (программы удаленного доступа) преступник может завуалировать под приложение интернет-банкинга и иное.

Кроме того, распространена следующая схема обмана: гражданину поступает звонок от «специалиста компании оператора сотовой связи («A1», «МТС», «Life») с использованием различных мессенджеров (WhatsApp, Viber, Telegram). В ходе телефонного разговора злоумышленник под предлогом обновления официального приложения, продления договора обслуживания и т.п., отправляет ссылку для скачивания вредоносного файла (формата «.apk»).

После скачивания и запуска указанного файла, производится установка приложения удаленного доступа внешне схожего с официальным приложением оператора сотовой связи. Установленное приложение обладает функциональными возможностями, предоставляющими доступ злоумышленнику к функциям мобильного телефона, в том числе камере, микрофону, файлам, хранящимся на устройстве, списку контактов, смс-сообщениям и др. Полученные сведения могут быть использованы для совершения хищения денежных

средств с банковских счетов и иных противоправных действий в отношении владельца мобильного телефона (завладение информацией и иное).

**Шестидесятидвухлетней минчанке позвонили в мессенджере "WhatsApp" представились специалистом компании "МТС". Под предлогом продления договора минчанка установила мобильное приложение "мой МТС". В последующем обнаружила, что с её карт-счета в Альфа-Банке были списаны денежные средства в размере 2 096 бел.рублей.*

**Пенсионерке посредством обычной телефонной связи позвонил неизвестный, представился сотрудником оператора сотовой связи "А1" и сообщил, что с номера заявительницы происходит спам-рассылка, в связи с чем он будет заблокирован. Далее неизвестное лицо переключило пенсионерку на представителя Департамента финансовых расследований. который обвинил ее в финансовом обеспечении военных нужд Украины. Заявительница сбросила вызов, после чего пришло СМС уведомление от "МТБанк" о том, что с БПК списаны денежные средства в общей сумме 3 700 бел.рублей. Заявительница пыталась связаться с одним из неизвестных посредством мессенджера "Telegram", в ходе общения он стал ей угрожать.*

Рекомендации:

✓ ни под какими предлогами не сообщайте посторонним персональные данные (паспортные данные), не предоставляйте информацию о реквизитах банковской карты (номере, сроке ее действия, ПИН-коде, CVV2/CVC2 коде) или одноразовые пароли, поступившие на мобильный телефон, даже если звонят лица, представляющиеся сотрудниками правоохранительных органов, медицинских и банковских учреждений, операторов сотовой связи, работниками коммунальных служб или телекоммуникационных компаний;

✓ не оформляйте кредиты по указанию третьих лиц;

✓ не проводите через банкоматы и иные устройства самообслуживания (включая систему дистанционного банковского обслуживания) никакие операции под психологическим давлением или по инструкциям, полученным по телефону или мессенджерам;

✓ не устанавливайте на мобильный телефон приложения по просьбе третьих лиц, даже если они настоятельно этого требуют;

✓ не становитесь курьером мошенников, путем собирания денежных средств у других граждан, попавших в неприятную жизненную ситуацию.

✓ при поступлении ЛЮБОГО сомнительного звонка, незамедлительно завершите разговор и обратитесь в милицию.

ПОМНИТЕ, сотрудники правоохранительных органов, медицинских и банковских учреждений, операторов сотовой связи, работники государственных организаций и предприятий, коммунальных служб или

телекоммуникационных компаний НИКОГДА не выясняют ваши персональный данные по телефону!

Для оформления заявок на оказание услуг по телефону указание идентификационного номера паспорта либо реквизитов банковской пластиковой карты НЕ ТРЕБУЕТСЯ!

Справочная служба «Белтелеком» - 123;
Справочная служба «Энергосбыт» (Минскэнерго) - (017)371 00 33
Справочная служба «Водоканал» - 119
Справочная служба «Мингаз» - 162
Контакт-центр Нацбанка – (017)375 20 02
Следственный комитет Республики Беларусь – (017)389 50 02
Комитет государственного контроля Республики Беларусь – (017)327 47 11
Департамент финансовых расследований (017)357 53 75

Управление по противодействию киберпреступности
криминальной милиции ГУВД Мингорисполкома