«Профилактика киберпреступлений, мошенничеств совершаемых с использованием информационно-коммуникационных технологий»

Состояние преступности в сфере противодействия киберпреступности.

На территории Гродненской области зарегистрировано преступлений в сфере противодействия киберпреступности:

2018 г. – 300 преступлений

2019 г. – 930

2020 г. – 2700

2021 г. – 1814

2022 г. – 1407

2023 г. – **1529** (из которых **1420** – хищения денежных средств: 1096 – совершенных путем модификации компьютерной информации, 301 – путем мошенничества и 23 – путем вымогательства).

За 1 полугодие 2024 года в сравнении с аналогичным периодом прошлого года произошел существенный рост по отдельным видам преступлений. В частности, со 101 до 665 возросло количество мошенничеств; с 14 до 40 увеличилось число вымогательств, с 5 до 47 преступлений по незаконному обороту средств платежа и инструментов (ст. 222 УК), с 2 до 11 преступлений, предусмотренных ст. 340 УК (заведомо ложное сообщение об опасности).

Как видно из статистики, как в 2022-2023 годах, так и в текущем году, на территории Гродненской области фиксируется большое количество хищений денежных средств граждан, совершенных с использованием информационно-коммуникационных технологий, большую часть которых составляют именно хищения (путем мошенничества (ст. 209 УК) и модификации компьютерной информации (ст. 212 УК).

Хищение денежных средств путем модификации компьютерной информации злоумышленниками совершается в результате получения доступа к банковскому счету с использованием переданных владельцем счета реквизитов банковской карты, путем доступа к системе интернет-банкинг или к мобильному устройству потерпевшего через удаленные программы, а также с использованием похищенной или потерянной банковской платежной карты.

Хищение **путем мошенничества** совершается в результате использования преступником, так называемых методов социальной инженерии, когда потерпевшего вынуждают под видом звонка от сотрудника банковского учреждения или правоохранительных органов добровольно осуществить перевод денежных средств для их сохранения на счете или с целью поимки мошенника, а также в качестве предоплаты за товар в фейковом интернет-магазине, за аренду жилья и т.д.

Зафиксированные факты **вымогательства** в Интернете в большей части связаны с высказыванием требований перевода денежных средств под угрозой распространения в сети интимных материалов, «попавших» в руки злоумышленнику в ходе доверительной переписки на сайтах знакомств, в социальных сетях, мессенджерах. Доступ к таким материалам злоумышленник

также может получить после взлома страниц в социальных сетях и в иных аккаунтах.

Наиболее распространенные схемы и способы, которые используют преступники для хищения денежных средств в сети Интернет.

1. **«Вишинг» -** метод социальной инженерии, заключающийся в осуществлении телефонных звонков гражданам (как правило в интернет-мессенджерах) от имени работников банковских учреждений, правоохранительных органов, когда злоумышленники сообщают гражданину, что какое-то лицо без ведома оформило на него кредит либо совершается попытка хищения денежных средств со счета.

Для отмены кредита, либо предотвращения хищения денежных средств со счета и поимки виновного необходимо срочно оформить новые кредиты на максимальную сумму платежеспособности, либо перевести деньги на «безопасный счет» или «защищенную ячейку». Для убедительности к данным звонкам «жертве» также начинают поступать звонки от имени работников Нацбанка, сотрудников ОВД и следователей, подтверждающих наличие проблемы, с целью убеждения осуществления переводов денежных средств и участии в мероприятии по выявлению преступника. Потерпевшему могут также высылаться в мессенджере фотографии служебных удостоверений, злоумышленники инструктируют как себя вести при оформлении кредита в банке. В данном случае действуют участники организованных групп. В ряде случаев таким образом мошенники убеждают граждан оформлять кредиты на крупные суммы, осуществить их перевод, в том числе имеющихся на счету денежных средств, на подконтрольные злоумышленникам счета, и похищают их. Преступники действуют настолько убедительно, что зачастую потерпевшие осуществляют переводы в течение нескольких дней, имея реальное время подумать над происходящим. Нередко злоумышленники также убеждают граждан устанавливать на мобильный телефон приложения для удаленного доступа к телефону (вы последнее время, в том числе представляясь работниками компаний сотовой связи), в ходе чего сами получают доступ к телефону и системам интернет-банкинг, и самостоятельно осуществляют хищение денежных средств со счета, в том числе дистанционно оформляя на граждан кредиты.

2. **Веб-сайты**, имитирующие различные **трейдинговые платформы** для заработка денежных средств на торгах. Спам реклама о данных сайтах распространяется повсюду в сети Интернет. Доверчивые граждане переходят по ссылке, не проверив историю и отзывы ресурса, вступают с так называемыми представителями биржи в переписку. Граждан убеждают в высоких доходах, чему способствуют содержащиеся на ресурсе красивые фейковые отзывы об эффективности торгов. Убеждают перечислять деньги на предоставленные номера банковских счетов, нередко на криптокошельки. Для убедительности создают «жертвам» личные аккаунты на данных сайтах, где якобы отображаются суммы внесенных денежных средств. А когда человек решает вывести «имеющие на счету» и вложенные деньги, начинается «история» о необходимости внесения

налога, страховки, компенсации и т.д., вынуждая потерпевшего вносить очередные суммы денег средств

4. Фишинговые сайты банков, театров и кинотеатров.

В сети Интернет существует ряд сайтов, имитирующих главные веб-страницы банковских учреждений и страницы интернет-банкинга. Желая зайти в приложение, граждане ищут страницу интернет-банкинга своего банка путем поискового запроса в браузере, что делать нельзя. Нередко в первых результатах поиска за названием аббревиатуры финансового учреждения кроется ссылка на фишинговый сайт, внешне ничем не отличающийся от оригинала (по наполнению, цвету, разделам и т.д.), но имеющий иной адрес в адресной строчке браузера. Отличаться он может даже одним символом от правильного адреса. Вводя на таком сайте логин и пароль владелец счета предоставляет доступ к интернет-банкингу, а это полный доступ к счету. Через считанные минуты денежные средства переводятся злоумышленником на иной счет.

Аналогично в интернете распространяются ссылки на поддельные сайты **театров и кинотеатров**. Для покупки билетов необходимо ввести реквизиты БПК и код подтверждения из СМС. Далее происходит хищение денежных средств с карт-счета с использованием реквизитов карты. Нередко покупке билетов предшествует переписка со случайным собеседником в социальной сети, мессенджере, на сайте знакомств.

5. Иные способы

– завладение деньгами в виде предоплаты по объявлениям об **аренде жилья**,

– завладение деньгами в ходе переводов денежных средств в социальной сети или в мессенджере обратившемуся в переписке «другу» с просьбой **одолжить денежные средства**, или переводы в качестве **пожертвований** на фейковые объявления,

– **завладение интимными** материалами с последующем вымогательством денежных средств за неразглашение информации.

<u>РЕКОМЕНДАЦИИ гражданам:</u>

- ни под каким предлогом **никому не сообщать полные** реквизиты банковской платежной карты, в частности 3 цифры с оборотной стороны карты, коды из SMS, паспортные данные, логин и пароль от интернет-банка. Не хранить их в открытом доступе, не пересылать в социальных сетях и мессенджерах. Данные реквизиты являются ключами к банковскому счету. Три цифры с оборотной стороны карты нужны лишь для подтверждения расходной операции;

- не переходить по подозрительным ссылкам

При поступлении звонков от имени работников банковских учреждений (правоохранительных органов) следует знать:

- работники банка не звонят в мессенджерах и не просят устанавливать программы для доступа к телефону;

- сотрудники банка могут лишь уточнить, действительно ли держателем карт-счета совершалась определенная расходная операция по счету. Сотрудники банков и правоохранительных органов не требуют оформления кредитов, в ходе телефонных разговоров участии в поимке злоумышленников, предоставления

паспортных и иных личных данных, реквизитов БПК, кодов из СМС, осуществления переводов денежных средств на иные счета;

- в случае малейшего подозрения на несанкционированные действия со счетом сотрудники банка самостоятельно заблокируют операцию и/или банковский счет.

При желании заработать в сети Интернет, необходимо помнить:

- ряд фейковых сайтов в сети Интернет позиционируют себя биржами/трейдинговыми платформами, коими не являются, нет никаких гарантий в заработке и исключении потери денежных средств;

- такие сайты могут быть созданы за считанное время из любой точки мира, найти их владельцев крайне затруднительно;

- абсолютное большинство таких сайтов имеют в Интернете крайне отрицательные отзывы, которые легко найти путем поисковых запросов в сети;

- фейковые биржи, как правило, созданы (зарегистрированы) не более года назад, а то и месяцы до начала функционирования, что легко проверить в сети Интернет;

- для заработка в сети Интернет нужны большие познания и опыт работы с официальными известными интернет-ресурсами.

При посещении аккаунтов интернет-магазинов, в частности в сети **«Инстаграм», следует знать:**

- ранее неизвестные интернет-магазины, работающие только по предоплате и предлагающие товары стоимостью ниже рыночной, исключительно с положительными отзывами – максимально высокий риск потери средств;

- фотографии имеющихся товаров на множестве разных фонов (в разных помещениях) – один из признаков фейкового магазина, данные фото скачаны в сети Интернет;

- подобные фейковые аккаунты легко создаются в считанные часы, отзывы и подписки искусственно накручиваются, их владельцы могут находиться в любой точке мира, что усложняет их установление;

- более безопасно осуществлять покупки в интернет-магазинах на известных и проверенных интернет-площадках (известных брендов);

- при онлайн-покупках рекомендуется не использовать основную банковскую карту, а оформить виртуальную и перед совершением покупки переводить на нее необходимую сумму;

При осуществлении доступа к системе интернет-банкинг помните:

- нельзя искать сайт интернет-банка путем поискового запроса в браузере. Адрес сайта банка (страницы интернет-банкинга) нужно знать и вводить «вручную» в адресной строке. А лучше добавить в список закладок браузера, или использовать мобильное приложение.

Общаясь в социальных сетях, сайтах знакомств, путем переписки в мессенджерах следует помнить, что за аватаркой друга или знакомого может скрываться иное лицо, пытающееся завладеть денежными средствами или личными данными.

При необходимости финансовых перечислений следует удостовериться в личности собеседника с использованием других каналов связи (личная встреча, телефонный звонок, звонок посредством интернет-мессенджера).

К сожалению, дать рекомендации о поведении в каждом возможном случае нельзя, но всем гражданам в любой ситуации следует не терять бдительность, обдуманно относится ко всему происходящему в сети Интернет. Ведь в большинстве случаев излишняя доверчивость и неосмотрительность самих граждан способствует совершению вышеуказанных преступлений.