Приложение № 1

Информация по предупреждению преступлений, совершаемых с использованием ИТТ

Использование современных информационных технологий в промышленной, торговой, банковской, научной, культурной, образовательной и других сферах общественной жизни детерминировало динамичный рост и качественное обновление компьютерной преступности, что создает новые угрозы для развития общества и государства. Обеспечение своевременности и эффективности предупредительной деятельности в сфере информационно-телекоммуникационных технологий во многом зависит от комплексного подхода к разрешению организационных, правовых и методических аспектов предупреждения преступлений данного вида.

На территории Омской области сохраняется сложная оперативная обстановка, связанная с имущественными преступлениями, совершаемыми бесконтактными способами. По итогам 2023 года зарегистрировано 7009 имущественных преступлений *(рост составил 52,2%, Россия +29,9%, СФО +46,5%)*, квалифицированных по главе 21 УК РФ «Преступления против собственности», совершенных с использованием информационно-телекоммуникационных технологий и сети Интернет. По итогам 3 месяцев 2024 года зарегистрировано 1452 преступления данного вида.

В прошлом году из общего числа «дистанционных» преступлений 26,3% совершены в отношении лиц пожилого возраста, 52,7% – в отношении женщин, 0,6% – в отношении несовершеннолетних. Размер причиненного материального ущерба составил более 1,5 млрд. руб.

В 2024 году преобладают следующие способы совершения дистанционных мошенничеств:

- под видом операторов компаний, предоставляющих услуги сотовой связи, преступники звонят жертве и сообщают, что срок действия договора об оказании услуг сотовой связи истекает и его необходимо продлить, в противном случае номер сотового телефона будет передан другому абоненту, либо предлагают сменить тарифный план, подключить дополнительные опции, заменить sim-карту;

- под видом будущего работодателя звонят жертве и в ходе телефонного разговора проводят собеседование, в котором просят кандидата заполнить анкету. При заполнении данной анкеты жертва сообщает злоумышленнику личные данные и номер банковской карты;

- мошенники находят своих жертв в социальных сетях или через объявления в сети интернет, предлагая открыть «брокерский» счет, обещая жертвам заработать значительные суммы денег за короткий промежуток времени. Инвестиции, сделанные подобным образом, не возвращаются. Ущерб отдельных граждан по такой схеме достигает нескольких миллионов рублей;

- телефонные мошенники для обмана используют не только звонки, но и sms-сообщения. Массовая рассылка позволяет охватить наибольшее количество аудитории, тем самым увеличить шансы на обман. Преступники, присылают sms-

сообщение с номеров сотовых телефонов близких, родственников, знакомых с просьбой занять определенную сумму денег, либо проголосовать в детском конкурсе за детей или племянников. За ссылкой для голосования, которую мошенники отправляют со взломанного аккаунта владельца, скрыт вирус, который им откроет доступ к гаджету жертвы;

- изучая официальные сайты ведомств и организаций, преступники собирают сведения о лицах, их возглавляющих, а также о лицах, работающих в их подчинении. На основе данных, собранных с использованием социальной инженерии, о реальных аккаунтах в мессенджерах («WhatsApp», «Viber», «Telegram»), преступники создают «фейковые» аккаунты, и от имени руководителей пишут сообщения их подчиненным с указанием о том, что им будут звонить сотрудники правоохранительных органов – МВД, ФСБ, следственного комитета, а также Центрального Банка России. По легенде преступников, необходимо выполнить какие-либо указания финансового характера по предотвращению оформления кредита, либо хищения денежных средств с банковского счета, с последующим переводом денежных средств на безопасный счет;

- оплата услуг по фейковому QR-коду. Преступники наклеивают поверх официального QR-кода свой, отсканировав код, деньги уходят на счет мошенников;

- с использованием публичных Wi-Fi сетей, пользователь подключаясь к сети получает сообщение о необходимости регистрации через аккаунт в Телеграмм. После регистрации и отправки кода мошенникам последние получают полный контроль над аккаунтом, а пользователь теряет к нему доступ;

- мошенники звонят абонентам и выдают себя за сотрудников страховых компаний, в частности тех, которые работают через ОМС. В ходе телефонного разговора злоумышленники утверждают, что срок действия медицинского полиса их собеседника истек, который теперь необходимо заменить. Сделать это разумеется можно только на платной основе. Основная задача мошенников получить доступ к личным данным жертвы и его сбережениям. В России полисы ОМС представлены в трех вариантах: бумажном, пластиковом и цифровом, которые действуют бессрочно;

- в App Store появились фейковые приложения Сбербанка, ВТБ-банка и Тинькофф Банка. Программы выполнены в стилистике банков с их логотипами. Запомните, в App Store нет приложений вышеуказанных банков. Это фишинговые приложения, главная цель которых украсть персональную информацию;

- злоумышленники обзванивают граждан, пострадавших от финанисовых пирамид *(в основном «ФИНИКО»*), представляются экспертами юридической компании и предлагают помощь вкладчикам в возврате денежных средств, которые последние вложили в финансовую организацию. Главная задача мошенников заставить человека поверить в возможности быстрого возврата денежных средств. Аферисты просят заключить договор якобы для вывода денежных средств, а затем прислать свои персональные данные. Согласно

легенде это необходимо для того, чтобы узнать где именно находятся денежные средства, которые пострадавшие ранее вложили в пирамиду. Позже с зарубежных номеров звонят лжесотрудники банков, рассказывают, что для вывода денежных средств необходимо прислать фотографию развернутого паспорта и оплатить страховку в размере 10% от суммы счета потерпевшего. При этом мошенники уверяют, что как только транзакция пройдет успешно данная сумма денежных средств вернется к клиенту. Иногда злоумышленники убеждают вкладчиков в необходимости заключения договоров на оказание платных юридических услуг. В подтверждении своих слов аферисты присылают копии поддельных распорядительных актов государственных органов.

Чтобы не оказаться жертвой мошенников ПОМНИТЕ:

1. Сотрудники Банков НИКОГДА не просят сообщить данные Вашей карты *(номер карты, срок ее действия, секретный код на оборотной стороне карты)*, ни при каких обстоятельствах никому их не сообщайте.
2. Избегайте телефонных разговоров с подозрительными людьми, которые представляются сотрудниками банков, не бойтесь прервать разговор, просто кладите трубку.
3. Никогда и никому не сообщайте пароли и секретные коды, которые приходят Вам в СМС-сообщениях от банков.
4. Сотрудники банков не просят Вас пройти к банкомату.
5. Не покупайте в интернет-магазинах товар по явно заниженной стоимости, это очевидно мошенники.
6. Никогда не переводите денежные средства, если об этом Вас просит сделать Ваш знакомый или родственник в социальной сети, возможно мошенники взломали его аккаунт. Для начала свяжитесь с этим человеком и узнайте действительно ли он просит у Вас деньги.
7. Не переходите по сомнительным ссылкам на неизвестные сайты.
8. Не устанавливайте на гаджеты сторонние приложения.
9. При звонке с неизвестного номера с просьбой о помощи близкому человеку не впадайте в панику, не торопитесь предпринимать действия по инструкции неизвестных людей. Под любым предлогом постарайтесь прервать контакт с собеседником, перезвоните родным и узнайте все ли у них в порядке.
10. В СМС и ММС сообщениях не открывайте вложенные файлы, не переходите по ссылкам, удалите подозрительное сообщение.
11. Обо всех обращениях подозрительных лиц, предлагающих возврат, компенсации и другие возможности получения денежных средств, сообщайте в правоохранительные органы.
12. Не верьте звонкам от так называемых сотрудников правоохранительных органов, следователей ФСБ России о том, что Вы являетесь подозреваемым (обвиняемым). Уведомление гражданина о том, что Вы являетесь подозреваемым (обвиняемым) осуществляется исключительно в письменном виде и вручается лично.
13. Не верьте предложению сотрудников банка о переводе денежных

средств на «безопасный счет». «Безопасных счетов» не существует.

14. Не используйте зарплатную карту для онлайн-покупок. Для этих целей заведите отдельную (дебетовую) карту и пополняйте ее на ту сумму, которая необходима для оплаты.

15. У сим-карт нет срока действия, договор на услуги мобильной связи является бессрочным.

16. Не привязывайте банковские карты к сайтам и сервисам. Если сайт взломают или произойдет утечка данных, то платежные реквизиты окажутся в руках мошенников.

17. Не верьте обещаниям злоумышленников гарантированного высокого дохода в короткие сроки. Не участвуйте в инвестиционных онлайн-проектах.

18. Если пришлось подключиться к общедоступной сети Wi-Fi используйте ее только для безопасных операций (посмотреть карту, погоду или почитать новости).

УОДУУП и ПДН УМВД России по Омской области