Информация
о зарегистрированных в 2024 году на территории автономного округа преступлений, связанных с использованием (применением) информационно-коммуникационных технологий (далее – IT-преступления).

В соответствии с информацией, предоставленной Управлением Министерства внутренних дел Российской Федерации по Ханты-Мансийскому автономному округу – Югре (далее – автономный округ),

За январь 2024 года в автономном округе зарегистрировано 509 хищений, совершенных с использованием информационно-телекоммуникационных технологий (далее – IT-преступления, дистанционные хищения), что составляет 29,6% от общего числа зарегистрированных преступлений (1719). В общем числе IT-преступлений зарегистрировано 350 дистанционных мошенничеств, 159 краж. Количество дистанционных хищений превысило показатели декабря 2023 года на 48 преступлений (461). Число жителей Югры, пострадавших от действий преступников, выросло с 398 до 489 человек. Размер материального ущерба, причиненного потерпевшим, составил более 85,9 млн рублей.

Потерпевшими от действий мошенников стали 15 работников учреждений здравоохранения, 12 работников учреждений системы образования, 2 государственных гражданских служащих автономного округа и 3 работника подведомственных учреждений исполнительных органов автономного округа.

Новые схемы мошенничества.

Взлом аккаунтов и использование аудиочатов.

«Злоумышленники начали изучать переписки и использовать голосовые сообщения для обмана - сначала преступники взламывают аккаунт пользователя, затем выбирают подходящего собеседника и пытаются войти в доверие, подняв старую тему, которую находят в переписке.

Во время беседы они сначала отправляют старые голосовые сообщения, чтобы не вызвать подозрений и создать впечатление, будто человек действительно разговаривает со своим знакомым. После этого мошенники вспоминают о деньгах и просят перевести им какую-то сумму. Чтобы не попасться на уловки злоумышленников, следует проверять информацию через дополнительные каналы связи.

В целях защиты от мошенничества специалисты советуют удалять голосовые сообщения из чатов после прослушивания.

Просьба обновить банковское приложение:

Мошенник представляется сотрудником банка и просит установить новое приложение, якобы предыдущее устарело или больше не поддерживается. Затем

злоумышленники присылают ссылку по СМС, которая направляет на обновленное приложение банка. На самом деле это приложение, которое крадет данные пользователя. При установке программы и подтверждении разрешений она крадет пароли и реквизиты карт.

Помните, банки рассылают информацию о новых версиях приложений только через официальные источники.

Опрос под видом партии «Единая Россия» за вознаграждение в 2500 рублей.

Мошенники предлагают скачать фейковое приложение с поддельного Google Play, после опроса о предстоящих выборах жертвам предлагается ввести данные банковской карты для получения вознаграждения.

Далее страница запрашивает доступ к СМС и контактам мобильного устройства. Мошенники получают возможность без ведома жертвы получить СМС с кодом подтверждения перевода.

Банковские приложения.

Мошенники создали два фейковых приложения «Тинькофф»: The MortgagePro app и «Тинькофф — Ваш выбор» для AppStore

Они открывают поддельный сайт банка и предлагают оформить карту после внесения своих персональных данных.

Этого делать ни в коем случае нельзя, иначе ваши данные попадут в руки мошенников

Обман пользователей Сбербанка через популярные приложения для обмена сообщениями.

Афера начинается с того, что мошенники создают поддельные аккаунты на различных платформах обмена сообщениями, копируя внешний вид Сбербанка. Затем они связываются с пользователями, представляясь представителями банка, и интересуются, обновлял ли пользователь недавно приложение мобильного банка. Если пользователь отвечает отрицательно, мошенники предлагают дождаться звонка специалиста, который поможет с обновлением.

На втором этапе преступники связываются с жертвой с другого аккаунта или даже из другого приложения для обмена сообщениями с возможностью обмена экранами во время видеозвонка. Эта путаница с различными "специалистами" необходима для того, чтобы дезориентировать пользователя и заставить его следовать инструкциям. Второй "сотрудник" утверждает, что звонит для идентификации клиента по биометрическим данным. Затем они настаивают на том, чтобы пользователь включил режим разделенного экрана. Это, по утверждению Сбера, позволит "роботизированной системе диагностировать счет".

Однако на самом деле функция разделения экрана позволяет злоумышленникам просматривать номера карт, остатки на счетах и SMS-коды банковских операций. С помощью этой информации мошенники могут получить

доступ к личному счету клиента из приложения на устройстве и украсть деньги или убедить пользователя перевести их на поддельный "безопасный счет".

Чтобы не стать жертвой этой аферы, необходимо быть осторожным при общении с незнакомыми людьми, которые предлагают помощь в обновлении приложений или проверке аккаунта. Не позволяйте незнакомцам смотреть на ваш экран и не сообщайте свою личную информацию. Сохраняя бдительность и применяя проактивный подход к защите своих данных, вы сможете эффективно противостоять этим современным угрозам, направленным на пользователей Сбербанка.

Аферисты в письме предупреждают, что человек каждый месяц будет перечислять в бюджет десятки тысяч рублей, если срочно не зайдет в личный кабинет и не подпишет заявление на отказ от платежей. Для отказа мошенники предлагают перейти по ссылке на поддельный сайт банка и там войти в личный кабинет.

Когда человек введет на странице данные для входа, они сразу попадут мошенникам. Благодаря этому преступники могут вывести все деньги со счета или оформить кредит на имя жертвы.

Простые советы помогут Вам избежать неприятных ситуаций:

- храните в тайне свою переписку, паспортные данные и код с карты;
- не отправлять предоплату, если не уверены в порядочности продавца;
- никому не сообщать коды из смс и пуш-уведомлений;
- игнорируйте ссылки на оплату, которые присылает собеседник.
- осуществляйте мониторинг сети «Интернет» на предмет наличия отрицательных отзывов, а так же даты регистрации сайта.
- осуществляйте покупку билетов на различный вид транспорта исключительно с помощью официальных приложений, размещенных в «App Store» и «Play Market», а так же на официальных сайтах авиа и ж/д компаний.

Важно помнить о нахождении в Интернете сайтов-двойников, которые могут иметь наименования, созвучные с официальными сайтами.
(нужно внимательно изучить весть сайт, перезвонить на телефон технической поддержки, уточнить у оператора всю информацию о предоставляемых услугах).

Отдел по вопросам общественной безопасности и профилактики правонарушений Администрации города Ханты-Мансийска