Отчет по числу совершенных IT-хищений в Ханты-Мансийском автономном округе – Югре за 9 месяцев 2024 года

Проблема краж и мошенничеств, совершаемых дистанционно с использованием информационно-телекоммуникационных технологий (IT-хищения), сохраняет свою актуальность для жителей Ханты-Мансийского автономного округа – Югры (далее –автономный округ).

За 9 месяцев 2024 года прирост числа совершенных IT-хищений составил 22,4% (увеличение с 4530 до 5546 фактов).

Число потерпевших от IT-хищений увеличилось на 25,8% (4799 человек).

Удельный вес IT-хищений в общем количестве всех совершенных преступлений в Югре преступлений достиг 32,8% (каждое третье преступление).

Общий материальный ущерб от дистанционных хищений превысил 2 миллиарда рублей (2,073).

В среднем за одни сутки в автономном округе совершается 20 IT-хищений (600

фактов в месяц), ущерб от которых составляет более 7 миллионов рублей (более 220 млн рублей в месяц).

Результаты опроса правоохранительными органами потерпевших граждан свидетельствуют о том, что более 90% пострадавших были осведомлены о потенциальной угрозе преступных посягательств и основных схемах, применяемых преступниками для обмана граждан.

Мошенники совершенствуют методы и схемы обмана граждан, в том числе используя технологии социальной инженерии.

При этом жертвами мошенников становятся все категории граждан независимо от возраста, образования, социального статуса и имущественного положения.

На территории города Мегиона только за последние 3 месяца 2024 года общий ущерб от хищений, совершенных с использованием информационно-телекоммуникационных

технологий составил 29 536 453 рублей. Наиболее популярными схемами являются:

• Сообщения руководителя в адрес подчиненных через приложения «Telegram»,
«WhatsApp», «Viber»

• Сообщения с просьбой перевести денежные средства через приложения «WhatsApp»,
«Telegram»;
• Продажа/Покупка вещей на «Авито», «Дром»;
• Переход по подозрительным ссылкам;
• Оформление на сайтах-двойниках квартиры, номера, покупка товаров;
• Перевод на лицевой счет продавца в приложениях «ОЗОН», «ВБ»;
• Продление договоров по абонентским номерам;
• Приложение для занятий брокерством, инвестиции;
• Перевод бонусов «СБЕР-спасибо» в рубли;
• Интим услуги.

В настоящее время основной рекомендацией безопасного поведения является – безоговорочное и безусловное прекращение дистанционного общения (по телефону, в мессенджерах, социальных сетях) если разговор с незнакомым собеседником переходит к необходимости передачи персональных данных, сохранению или преумножению денежных средств, угрозам привлечения к ответственности за невыполнение требований.

Более радикальный, но в современных условиях оправданный вариант – не отвечать на телефонные звонки с незнакомых номеров и любой входящий звонок или сообщение оценивать критически, поскольку с развитием IT-технологий прогнозируется увеличение фактов мошенничества с применением дипфейков (технологический синтез изображения или голоса иного лица).

Управлением по организации борьбы с противоправным использованием

информационно-коммуникационных технологий МВД России информация о применяемых новых схемах мошенничества размещается на телеграмм-канале «Вестник Киберполиции России»: https://t.me/cyberpolice_rus.

Для получения более подробной информация по профилактике IT-преступлений, популярных схемах рекомендуем подписаться на следующие источники: