Опубликовано: 6 марта 18:55 ИСТОЧНИК: НАРОДНАЯ ГАЗЕТА

Цифровая охота. В Беларуси усиливают защиту от кибераферистов

Каждый день в новостной ленте появляются сообщения о том, что мошенники обвели вокруг пальца очередную жертву. В 2025 году они похитили у белорусов более 54 миллионов рублей. И хотя общее число зарегистрированных киберпреступлений снизилось до 9,8 тысячи (на 1,3 тысячи меньше, чем годом ранее), поводов для самоуспокоения нет. Схемы становятся сложнее, атаки — точечнее. В ответ правоохранительные органы, банки и заинтересованные ведомства внедряют новые механизмы противодействия, совершенствуют антифрод-системы и борются за должное хранение организациями наших персональных данных, дабы они не попали в руки преступников.

Александр Лукашенко:

— Борьба с киберпреступлениями входит в число ключевых и весьма непростых задач для правоохранителей стран СНГ. И она актуальна для всех стран. Ведь после начала проведения СВО активизировались центры мошенников, в том числе и кол-центры, действующие на территории Украины. Также возросло число попыток дестабилизации работы госорганов путем заведомо ложных сообщений о минировании важнейших государственных объектов.

8 августа 2024 года, во время встречи с участниками заседания Совета министров внутренних дел государств — участников СНГ.

Под видом инвестиций

Более пяти лет в Минске действовали два крупных мошеннических кол-центра. Они работали по принципу так называемой форекс-кухни. Клиентам обещали высокий доход от инвестиций в несуществующие финансовые компании. При такой схеме компания лишь имитирует торговлю на финансовых рынках: на платформе отображаются графики, котировки, отчеты, а баланс инвестора якобы растет. На самом же деле средства не участвуют в реальных сделках — они оседают на счетах преступников и в их криптокошельках.

В качестве крючка мошенники создали боле 800 сайтов. Они рассчитывали на людей, интересующихся пассивным заработком, рассказывает начальник 5-го управления (по Минску) ГУБОПиК МВД Сергей Новик:

— После этого с ними связывались сотрудники кол-центра под видом специалистов по брокерским услугам и предлагали консультацию. Сумма первоначального депозита составляла 500 долларов. После его внесения клиенту демонстрировали фиктивную прибыль. Как только человек пытался вывести средства или переставал пополнять счет, начинались проблемы: якобы недостаточная сумма для вывода, необходимость доплаты комиссии или налога. В итоге, когда извлечь из человека было уже нечего, связь с ним прекращали. При этом люди нередко не осознавали, что стали жертвами мошенничества, полагая, что просто проиграли на финансовых рынках.

К слову, «бизнес» приносил немалые деньги: ежемесячный оборот одного из кол-центров составлял от 600 тысяч до 2 миллионов долларов.

Внутренняя кухня

Как же этим кол-центрам удавалось так долго оставаться вне поля зрения милиции? Дело в том, что они скрывались за вывесками организаций, оказывающих телефонные и справочные услуги. Штат весьма внушительный: помимо операторов (менеджеров по обзвону), в него входили сотрудники технической и финансовой поддержки, бизнес-тренеры, HR-менеджеры, клоузеры (менеджер, завершающий сделки), полиграфологи и даже штатная охрана.

— *Подбор кадров кол-центра осуществлялся в том числе через официальные площадки. С кандидатами проводили собеседование, после чего направляли их на двухнедельные курсы. Во время или после обучения соискателей проверяли с использованием полиграфа. Особое внимание уделялось их отношению к правоохранительным органам и отсутствию моральных качеств,* — подчеркивает Сергей Новик. — *По окончании курсов кандидаты сдавали зачеты. Все работали под псевдонимами.*

Заработная плата рядовых сотрудников начиналась от 500 долларов, в ретеншн-отделе (отвечает за клиентскую базу) — от тысячи долларов, однако фактически многие получали от 3 до 4 тысяч долларов в месяц. Руководитель двух офисов зарабатывал по 5 тысяч долларов.

Для защиты от «нежелательных гостей», как участники кол-центров называли сотрудников милиции, в офисах были установлены тревожные кнопки. Они позволяли мгновенно отключать все компьютеры от сети питания, прекращать доступ как к внутренним, так и к внешним информационным ресурсам, блокировать доступ к интернету.

В середине февраля сотрудники правоохранительных органов провели масштабную операцию, ликвидировав эти кол-центры. Изъяли более 790 тысяч рублей. Задержаны 55 человек — 45 мужчин и 10 женщин.

Если раньше мошенники напрямую представлялись сотрудниками КГБ или МВД, сообщали о якобы оформленных на человека кредитах и убеждали перевести деньги на «безопасные счета» либо поучаствовать в «спецоперации», то теперь схема изменилась. Люди стали чаще распознавать обман, поэтому преступники адаптировали подход.

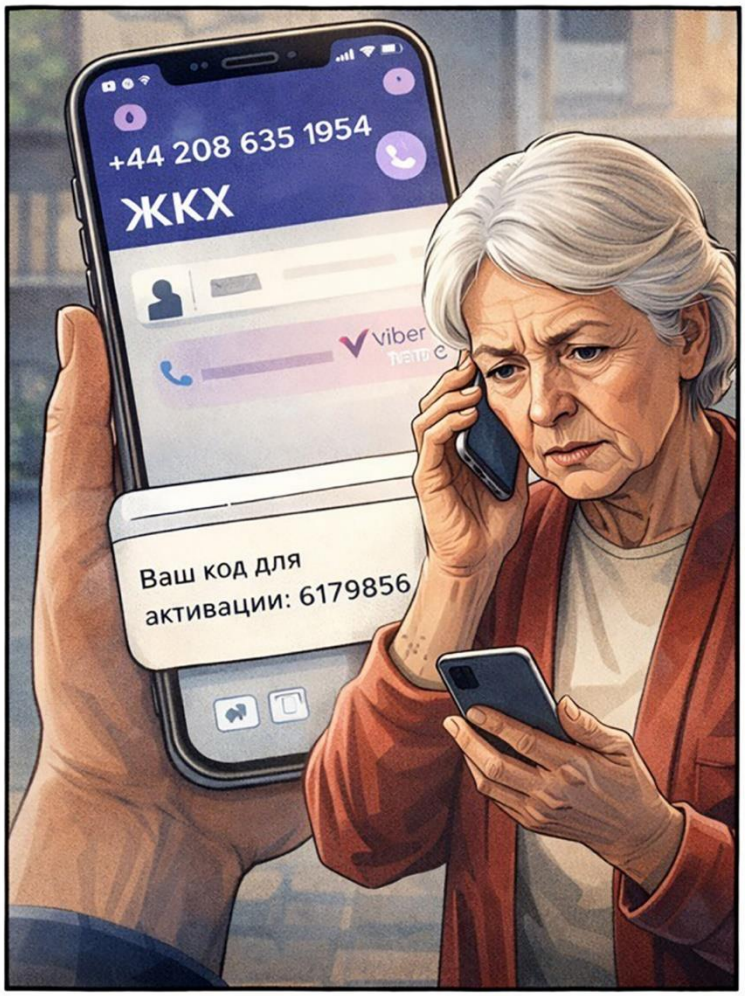
Сегодня львиная доля киберпреступлений — это так называемые двухэтапные звонки. В обновленной схеме сначала проводится разведка: злоумышленники связываются с жертвой под видом сотрудников коммунальных служб, операторов связи, «Белтелекома».

— Например, звонят якобы из водоканала и сообщают: «Вам направлялись письма о продлении договора. Поскольку вы с нами не связались, давайте решим вопрос дистанционно. В противном случае договор будет признан недействительным и у вас отключат воду», — рассказывает заместитель начальника управления по противодействию киберпреступности ГУВД Мингор-исполкома Дмитрий Шевелев. *— Опасаясь остаться без услуги, человек соглашается. У него уточняют личные данные: фамилию, имя, паспортные сведения, адрес, контактную информацию.*

После этого начинается вторая фаза — атака.

Жертве звонят уже якобы из правоохранительных органов и обвиняют в незаконных финансовых операциях или сообщают, что на ее имя оформлены заявки на кредиты. Человек пугается, так как этого не делал и боится влезть в долги. Дальше преступники играют на этом. Они предлагают «опередить мошенников»: самостоятельно взять кредиты и перевести средства на «безопасный счет».

— Под предлогом совместной «спецоперации» по поимке преступников человека убеждают оформить займы и перечислить деньги злоумышленникам, — поясняет Дмитрий Шевелев. *— Дальше события могут развиваться по-разному. Если жертва ведется, мошенники могут «записать» ее в курьеры. Человек пойдет и заберет деньги у такого же обманутого, думая, что делает благое дело.*



Кирпич вместо телефона

На втором месте по количеству пострадавших — псевдопродажи через соцсети и торговые площадки. Особенно обострилась ситуация накануне 8 Марта. Люди заказывают цветы через аккаунты якобы цветочных магазинов, переводят предоплату и остаются ни с чем.

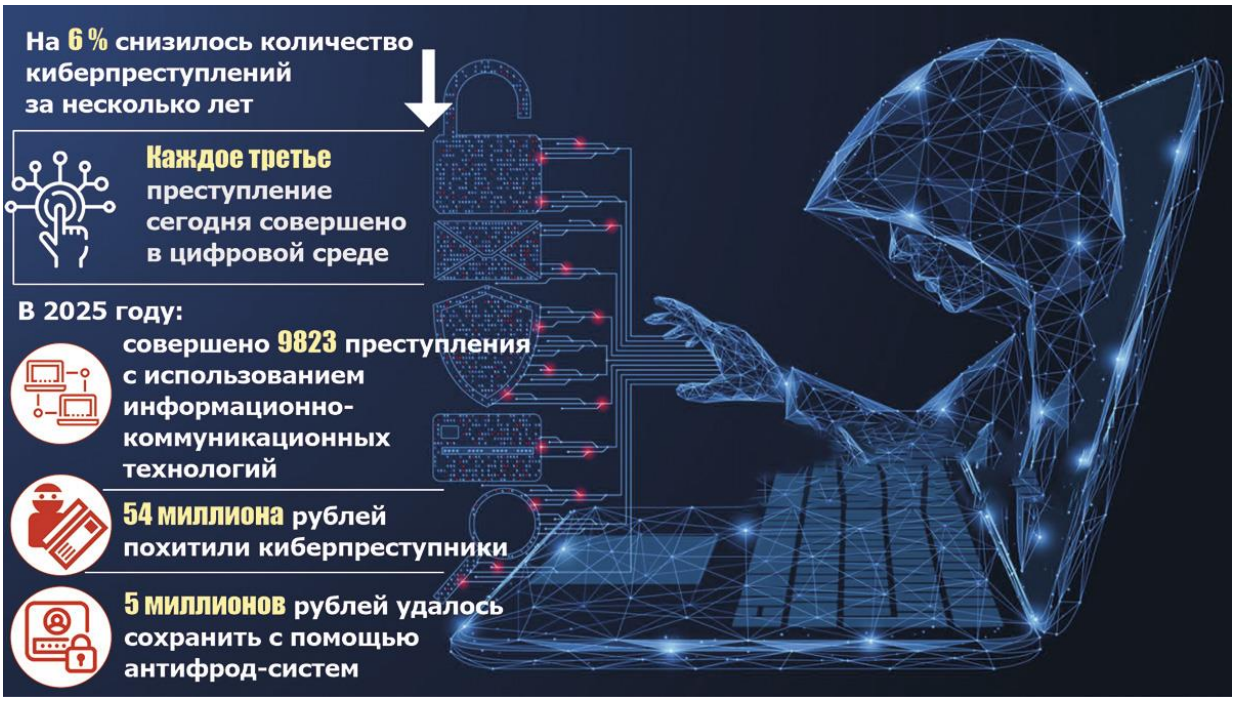
Кроме того, в последнее время участились случаи блокировки айфонов с последующим вымогательством денег.

— *Преступники ищут жертв через игровые сообщества в соцсетях, группы поиска работы. Дальше налаживают с ними общение. Когда доверие установлено, жертве предлагают войти в подставную учетную запись Apple ID. Если речь о ребенке, предлогом может быть доступ к прокачанному игровому аккаунту. Взрослых чаще «ловят», притворяясь работодателями. Предлагают авторизоваться в «корпоративной» учетной записи,* — отмечает собеседник.

Жертва добровольно выполняет выход из своего Apple ID и входит в

чужую учетную запись. Телефон превращается в «кирпич», на экране блокировки появляется сообщение с требованием выкупа.

— *Совет один: не авторизоваться в чужих учетных записях, кем бы ни представлялся собеседник. В противном случае вернуть контроль над устройством практически невозможно,* — уверяет Дмитрий Шевелев.



Плюс к обороне

С 2024 года в каждом банке организованы подразделения по выявлению мошеннических операций — антифрод-подразделения, которые работают 24/7. В прошлом году благодаря этому удалось предотвратить хищение около 5 миллионов рублей. Эти средства были возвращены клиентам.

Система защиты совершенствуется. С 1 июля все банки в стране перейдут на единые стандарты защиты финансовых операций клиентов.

— *Это позволит снизить риски кражи со стороны мошенников,* — отмечает заместитель начальника управления защиты информации Национального банка Дмитрий Курило. — *Первый стандарт касается антифрод-сис-тем оценки операций. Все банки страны внедрят сессионный и транзакционный антифроды. Система будет анализировать каждый вход клиента в мобильный банк: способ авторизации, время входа, устройство. Например, если пользователь обычно заходит днем с использованием биометрии, а затем авторизуется ночью через ввод пароля, операция может быть*

признана подозрительной.

При совершении нетипичной операции, например переводе средств в другую страну или на ранее неизвестный счет, система автоматически обратит на это внимание, приостановит транзакцию либо запросит дополнительное подтверждение.

Еще один механизм защиты — блокировка номеров, с которых совершаются мошеннические звонки. Этой работой занимается Следственный комитет совместно с Министерством связи и информатизации, операторами связи.

Кроме того, правоохранительные органы блокируют фишинговые интернет-ресурсы. Если ресурс зарегистрирован в Беларуси, его работа полностью прекращается. Если же он создан за рубежом, доступ к нему блокируется с территории нашей страны. В прошлом году было выявлено более 14 тысяч таких сайтов.

ТОЧЕЧНАЯ АТАКА

Наша страна вторая в СНГ по числу кибер-атак. И речь не только о мошеннических звонках, но и о более серьезных угрозах. Банки, логистика, телеком и госуслуги подвергаются фишинговым атакам, внедрению вредоносного ПО и шантажу с использованием программ-шифровальщиков. Здесь финансовые потери могут исчисляться в совершенно иных суммах.

— *Чаще всего атаки на организации и компании нацелены либо на то, чтобы снизить конкурентоспособность организации на рынке, либо на то, чтобы добыть какие-то данные из информационной системы,* — рассказывает заведующий кафедрой защиты информации БГУИР кандидат технических наук Ольга Бойправ. — *В первую очередь речь о DDoS-атаках. Они направлены на то, чтобы вызвать отказ в обслуживании. Сервер обрабатывает массу бесполезных запросов, поступающих от ботнета, и перестает отвечать реальным пользователям. Это удар по репутации и работе компании. К слову, самой масштабной DDoS-атаке за 2025-й подверглась облачная платформа Microsoft Azure. Мощность достигала 15,72 терабита в секунду, атаковали более 500 тысяч IP-адресов.*

Вторая форма атаки — фишинговая рассылка. Она нацелена на то, чтобы перехватить пароли от учетных записей пользователей информационной системы, дальше, уже применяя эти данные,

планировать другие кибератаки на эту систему. Классика жанра — в письме ссылка на внешний ресурс. С виду он может быть похож, например, на ту же самую страницу для ввода логина и пароля в системе Google либо корпоративной почтовой системе. Никаких подозрений у пользователя это, к сожалению, как правило, не вызывает, он вводит свои учетные данные, а они попадают к мошеннику.

— Пример другого варианта «вредоносной» почты — письмо с текстом «срочно проверить дебиторскую задолженность, информация в прикрепленном файле», где как раз таки вредоносный программный код, который шифрует активы информационной системы. Такая форма «вредоносной» рассылки придумана для того, чтобы вымогать с организации деньги, — отмечает собеседница.

НАЦЕЛИЛИСЬ НА ДЕТЕЙ

Нередко жертвами киберпреступников становятся пожилые люди. Однако в последнее время все чаще в поле зрения мошенников попадают дети. По словам заместителя начальника управления по противодействию киберпреступности ГУВД Мингорисполкома Дмитрия Шевелева, бывает, злоумышленники изначально не знают, что попадут на несовершеннолетних:

— У них есть определенные скрипты. И понимая, что на том конце провода ребенок, они выстраивают соответствующую линию коммуникации. Один из распространенных сценариев — запугивание уголовным делом в отношении родителей. Чтобы «спасти» близких, школьника принуждают передать крупную сумму денег и строго запрещают рассказывать об этом кому-либо, включая родителей и друзей.

Так, 11-летнему минчанину позвонили лжесотрудники сотовой связи и поинтересовались, с кем он живет. Затем с ним связались другие мошенники и пригрозили школьнику, что если он не будет их слушаться и выполнять задания, то родителей арестуют, а его самого отправят в детдом. Ребенок испугался и поверил.

На протяжении нескольких недель преступники держали мальчика на связи и убеждали, что наблюдают за ним. По их указанию школьник попытался открыть домашний сейф, но не смог. Тогда ему велели вынести сейф на общий балкон и снять весь путь на видео. В тот же день за ним пришел курьер. Как оказалось, он тоже стал жертвой преступников и был убежден, что помогает правоохранительным органам.

Еще один случай произошел в декабре: 12-летнюю школьницу фактически сделали курьером мошенников. Она вместе с подругой познакомилась в интернете с якобы ровесником, который для встречи попросил прислать геолокацию. Вскоре с девочками связались неизвестные и заявили, что их данные оказались в руках преступников, а семьи находятся в опасности.

Затем поступили сообщения якобы от следователя с угрозами ареста родителей. Чтобы этого избежать, одна из девочек собрала семейные сбережения, забрала деньги у подруги, сложила около 50 тысяч рублей в эквиваленте в рюкзак и передала их незнакомцу.

ЛИЧНОСТЬ ПОД ЗАЩИТОЙ

Основной источник информации для мошенников — слитые на теневые форумы базы данных. В них можно найти имена клиентов, номера телефонов, адреса, даты рождения, а порой и пароли с паспортными данными. Эти утечки становятся настоящим кладом для зло-умышленников, использующих их для обмана и шантажа. Чтобы навести порядок в этой сфере и обеспечить ответственное обращение с персональной информацией, в 2021 году в стране был принят Закон «О защите персональных данных». Сейчас идет работа над его совершенствованием.

— *За последние три года сократилось количество утечек персональных данных. Кроме того, бизнес сегодня рассматривает вопросы защиты личной информации как конкурентное преимущество,* — подчеркивает директор Национального центра защиты персональных данных Андрей Гаев. — *Однако проблемные ситуации остаются. Речь идет, в частности, об избыточном сборе данных и необоснованной видео- и аудиофиксации. Фактически каждая вторая жалоба, поступающая в центр, связана с этим. На практике встречаются случаи тотального видеонаблюдения в местах, напрямую связанных с личной сферой. Например, когда человек приходит за оказанием медицинских услуг, во время манипуляции осуществляется его съемка либо производится видео- и аудиозапись в местах приема пищи, переодевания.*

Новые вызовы возникли и из-за технологии искусственного интеллекта. Андрей Гаев отметил, что наряду с очевидными преимуществами ИИ создает риски, связанные с подменой личности, дипфейками и манипуляцией данными:

— *Искусственный интеллект требует внимательного правового регулирования, поскольку напрямую затрагивает вопросы сохранения человека в цифровом мире.*

yankovich@sb.by

Изображения сгенерированы ИИ.

Александра ЯНКОВИЧ