старший следователь по особо важным делам Следственного комитета Республики Беларусь

дмитрий бродко

следователь по особо важным делам Следственного комитета Республики Беларусь

Александр ластовский

старший оперуполномоченный по особо важным делам главного управления по противодействию киберпреступности министерства внутренних дел республики беларусь

сергей майсейшин

начальник отдела реагирования на компьютерные угрозы управления защиты информации национального банка республики беларусь

цифровая личность и цифровая гигиена

Александр ластовский

Основная причина роста преступлений в киберсфере — недостаточная цифровая грамотность граждан.

Мы живем в эпоху цифрового мира. Поэтому все то неприятное, что с нами может случиться в реальном мире, может произойти и в виртуальном. Если обратиться к статистике, то количество преступлений, совершенных в киберсфере, растет.

К сожалению, таких преступлений очень много и главная их причина - недостаточная цифровая грамотность наших граждан. Передать на улице незнакомцу банковскую карточку звучит дико, но почему-то в цифровом мире мы делаем это совершенно спокойно – сообщаем по телефону личные данные.

С начала этого года совершено порядка 10 тысяч преступлений, причем 90 % из них приходятся на так называемые мошеннические звонки.

Под видом, например, сотрудника правоохранительных органов неизвестные пытаются выманить у граждан реквизиты доступа к их банковским счетам.

кибермошенничество

иван судникович

Атака идет с территорий других стран, где находятся организаторы преступных групп.

Были созданы специальные подразделения милиции, в последующем в Следственном комитете -

специальные подразделения оперативных сотрудников, которые занимались раскрытием и расследованием этих преступлений. То есть решили основной вопрос – кадровый, начиная с центральных аппаратов и заканчивая областями, благодаря чему удалось сдержать рост преступности.

Ситуация начала 2000-х отличалась от текущей тем, что преступники в основном находились на территории Беларуси, России и Украины - это международные преступные группы, которые атаковали страны Европы и Америку. В то время был получен колоссальный опыт раскрытия данных преступлений, который мы транслируем на нынешнюю ситуацию.

Первые киберпреступления были совершены в 2000-х годах. Лавинообразный рост начинается с 2006 года. За четыре года (2006-2009 гг.) рост составил 700%.

Сегодня ситуация меняется. С 2010 года мы сдерживали количество киберпреступлений на уровне 2,5 тыс. и начиная уже с 2017-2018 года опять идет лавинообразный рост, который сопоставим с уровнем 2000-х, но другая ситуация. Уже не мы защищаем богатые страны, а уже другие страны атакуют нас. Большинство атак идет с территории Украины и России. С 2018 года по 2020-й преступность в данной сфере выросла в 10 раз.

ДИНАМИКА КИБЕРПРЕСТУПЛЕНИЙ

В первую очередь систематизируются все сведения по профильным уголовным делам в республике, то есть вся информация, которая используется преступниками. В последующем посредством данных аналитических систем она анализируется, и специалисты выявляют гидру преступной группировки.

Атака идет с территорий других стран, где находятся организаторы данных преступных групп, они занимаются подбором определенного персонала, созданием call-центров, которые названивают белорусам, выявляют банковские карточки, и мы работаем над тем, чтобы этот процесс остановить. Но они постоянно совершенствуют свою деятельность.

Сегодня у нас новые вызовы, и если мы не примем никаких мер, то к 2025 году мы получим около 100 тыс. киберпреступлений. Поэтому разрабатываются различные способы противодействия. В частности, начинаем активнее использовать аналитические программы, которые разрабатывает Следственный комитет. В перспективе они позволят нам автоматизировать процесс сбора данных для того, чтобы раскрывать системные преступления республиканского масштаба. В ручном режиме обработать эти данные уже невозможно.

О самом крупном киберпреступлении в истории

иван судникович

В Беларуси подставному лицу, принимающему на свои счета похищенные деньги, грозит лишение свободы до 10 лет.

Дроп - это подставное лицо, низшее звено в иерархии интернет-мошенников. Наиболее часто его услуги нужны для получения теневых доходов, в том числе в результате мошенничества с пластиковыми картами.

Хотелось бы обратиться к гражданам, кто намерен какие-то легкие деньги получить за продажу своих карточек либо за то, чтобы на ваш счет перевели какие-то непонятные деньги и вы их сняли. Уже имеется уголовная ответственность за это. Поэтому передали с корыстной целью, продали свои реквизиты, поучаствовали, даже если вы якобы не понимаете, что они в преступных целях используются, сегодня уголовная ответственность введена - ст. 222 ("незаконный оборот средств платежа и инструментов"). Наказание на срок от 3 до 10 лет лишения свободы.

Они уже выходят на наших граждан для того, чтобы они принимали на свои счета эти похищенные деньги. Их называют подставные лица либо на нашем сленге на "дропы". То есть есть дроповоды, которые организовывают их деятельность, и дропы, наши граждане, которые дают свои реквизиты и снимают уже похищенные деньги, передают эти деньги переносчикам, которые потом перемещают их через границу, либо через криптовалюту переводят организаторам.

Как правило, реквизиты одной банковской карточки стоят для дропа не более Br30-Br50. По сравнению с предполагаемым сроком заключения это не такая и высокая цена. Я думаю, в этой ситуации мы сдержим этот рост. Поскольку правоохранительные органы уже ориентированы именно на отработку этих подставных лиц, которые фактически спонсируют оргпреступность на территории других стран. Поэтому предупреждаю: кто думает либо кому предлагают заработать таким образом деньги - не идите на это. Вас ждет уголовная ответственность.

ЦИФРОВАЯ ГРАМОТНОСТЬ

ПРАВИЛА

01

Не сообщайте в телефонной переписке свои финансовые реквизиты

Банки, правоохранительные органы никогда не общаются с гражданами по интернет-телефонии. То есть никогда не звонят через Viber, WhatsApp, Telegram. Поэтому, если такой звонок поступает вам, это стопроцентно мошенник.

ПРАВИЛО

02

не переводите деньги по интернет-переписке

Никогда не переводите деньги, если кто-то просит вас это сделать в интернет-переписке (близкие, знакомые, друзья), пока вы не уточните эту просьбу при личной встрече либо посредством телефонного звонка.

ПРАВИЛО

03

используйте три банковские карточки

Первая банковская карточка должна быть как расчетная. Вы ее используете при оплате в магазинах, на заправке и так далее. Вторая карточка - виртуальная, которую вы используете при оплате в интернет-магазинах, переводя на нее определенную сумму. Вы можете ее закрыть, открыть, перевыпустить. И третья карточка - накопительная, где вы храните свои накопления. И вы ее получили в банке, закрыли в свой сейф и никогда не используйте ни при платежах в интернете, ни в магазине.

характеристика потерпевших

ДМИТРИЙ БРОДКО

Жертвами кибермошенников чаще всего становятся женщины в возрасте старше 55 лет.

В этом году Следственный комитет проанализировал факты хищения денежных средств у организаций посредством подмены банковских реквизитов и подготовил методические рекомендации. Есть такая тема, когда ложное письмо приходит на корпоративную почту, от якобы контрагента, который находится за рубежом, что у них изменились реквизиты счетов. На основании этого Следственным комитетом подготовлены конкретные указания, что делать в таких случаях, какие степени защиты должны быть установлены, какие антивирусники.

В Следственном комитете провели анализ совершения преступлений по различным направлениям. Анализ социально-демографических характеристик потерпевших - это женщина в возрасте старше 55 лет, как правило, пенсионерка. Соответственно, это наши мамы и бабушки, которым мы дарим телефоны, подключаем социальные сети, но не объясняем, как правильно ими пользоваться. Элементарная цифровая грамотность, цифровая безопасность пенсионерам не разъясняется. Постоянно повторяется "не передавайте реквизиты банковских карт, бросайте трубку, если это подозрительный звонок". Но, к сожалению, люди продолжают поддаваться на уловки преступников.

О схеме "человек посередине"

Сергей майсейшин

В Беларуси по-прежнему распространен телефонный фишинг.

Основную кассу кейсов, связанных с мошенничеством, составляют инциденты, связанные с телефонным мошенничеством. Это пришло к нам около двух с половиной лет назад и, как показывает практика, не уходит. Люди продолжают вестись на разводы, схема не меняется, немного меняются скрипты разговора (в начале представлялись сотрудником банка, специалистом, потом был милиционер, потом работник Национального банка, потом появилась история с расследованиями). У нас фиксируются случаи с установкой программного обеспечения, которое позволяет удаленно контролировать устройство. Это все некий результат того, что человеку дозвонились и ему внушили, что ему нужно делать.

Нужен комплексный подход и совместная деятельность по противодействию этим преступлениям. Все упирается в цифровую грамотность.

Viber выпустил обновление в настройках, которое блокирует возможность дозвониться человеку

не из вашей телефонной книги.

Это отличная вещь. Если все бы ее применили, то телефонное мошенничество на какой-то период приостановилось, пока бы мошенники, грубо говоря, не нашли другой мессенджер.

Александр Ластовский

Сейчас наша цифровая личность полностью завязана на цифровой мир. Некоторые используют интернет в своих негативных целях. Например, был вал сообщений о ложной опасности. Я сейчас не говорю о телефонном терроризме, а именно о сообщениях, поступающих через электронную почту, мессенджеры на различные электронные почты предприятий. Хотелось бы предупредить тех людей, которые этим занимаются – существует международная помощь по делам о подобном терроризме. То есть правоохранители всех стран взаимодействуют в оказании взаимопомощи по выявлению и экстрадиции виновных лиц. Надо понимать, что в настоящее время понятие анонимности относительное по подобным сообщениям и существует уголовная ответственность.

Иван Судникович

Киберпреступники сегодня используют два способа. Первый - получить доступ к банковскому счету и перевести с него деньги. Чтобы это предотвратить, Национальный банк внедряет определенные инструменты, которые позволяют выявить, что это не владелец переводит средства и заблокировать операцию. Но чаще злоумышленники пользуются вторым, самым простым способом - в телефонном разговоре убеждают жертву перевести деньги на счет злодея. И здесь уже аналитической системе банков крайне сложно работать, так как переводит деньги сам владелец и какие-то отклонения от норм система не может зафиксировать. И здесь нам нужна помощь граждан.