От чего зависит защита персональных данных

Цифра безопасности

Охота за личными сведениями приобретает в виртуальной среде пугающие масштабы. На выуживание паролей, кодов, фотографий, сканированных копий паспортов нацелены мошенники, хакеры, криминальные посредники. В Беларуси многое делается для того, чтобы пресечь этот преступный интернет-бизнес. Что зависит от правоохранительных органов, а о чем должны побеспокоиться сами граждане?

Александр Лукашенко:

— Следует тщательно проработать вопрос защиты информации, а также принять все меры для недопущения уязвимости системы. Одновременно правоохранительным органам нужно активизировать деятельность по пресечению преступлений в сфере высоких технологий: проблема архиважная.

17 августа 2021 года, на совещании с руководством Совета Министров во Дворце Независимости.

На пароль надейся

37-летняя минчанка Ольга была шокирована, узнав, что ее страницу в Instagram взломали и разослали ее друзьям письма с призывом помочь ей собрать деньги на лечение сына. Сперва позвонила перепуганная родственница и сказала, что готова перечислить средства на указанный счет. Ольга ринулась в соцсеть. Но не тут-то было. Страничка не открывалась, пароль неверный. Оказывается, ей на почту ранее пришло сообщение, что осуществлен вход в ее аккаунт с постороннего устройства. Женщина стала писать знакомым в других мессенджерах, чтобы не перечисляли деньги, так как это уловка аферистов. Однако некоторые уже успели отозваться и перевести.

Чаще всего подобные взломы делаются с целью шантажа, фишинга или спама. Интернет — кладезь для мошенников: там хранится и личная информация, и переписки, и фотографии… В стране ежегодно фиксируются сотни преступлений против информационной безопасности. Довольно много бытовых случаев, когда бывшие возлюбленные из чувства мести получали доступ в аккаунт партнера и вели переписку от его лица. Или же сохраняли себе пароли и логины электронной почты, чтобы иметь к ней доступ и видеть, с кем ведется переписка. Следует помнить, что эти действия могут повлечь за собой уголовное наказание.

Со стороны пользователей стоит понимать, что безопасно выкладывать в сеть, а что не стоит. Заведующий кафедрой защиты информации БГУИР профессор Тимофей Борботько обращает внимание, что нередко люди фотографируют свои банковские карты, паспорта и другие важные документы, а снимки сбрасывают в галерею смартфона, отправляют близким через мессенджеры и соцсети, загружают в облачные хранилища:

— Вроде удобно — нужная информация всегда под рукой. Но это таит большую опасность. Ведь все, что попадает в интернет, остается в нем навсегда. Чем и могут воспользоваться преступники.

YTIMG.COM

Тысячи строк

В главном управлении по противодействию киберпреступности МВД с начала года зарегистрировано около 8 тысяч киберпреступлений, 80 % из них — фишинг, вишинг. То есть когда у мошенников есть информация о вас. Так называемые строки с персональными сведениями продаются и покупаются в DarkNet или Telegram-каналах. Цена может достигать тысячи долларов. Понятно, чем база больше, полнее, тем она дороже.

— Купить можно не только личную информацию — Ф.И.О., номера мобильного и домашнего телефонов, паспортные данные, но и банковские сведения — остаток на счете, дата последней операции и так далее, — рассказывает Алексей Новаш, заместитель начальника главного управления по противодействию киберпреступности МВД. — *Также стоимость данных зависит от их свежести. И зачастую они используются для преступных действий. Возьмем так называемых телефонных мошенников. Чем больше они знают о клиенте, тем им проще вызвать доверие и вынудить жертв дать интересующую аферистов информацию.*

Большинство мошенничеств сегодня построены на методах социальной инженерии. То есть это чистая психология, воздействие на сознание, чтобы подвигнуть человека совершить определенные действия, отключая рациональность мышления, логику.

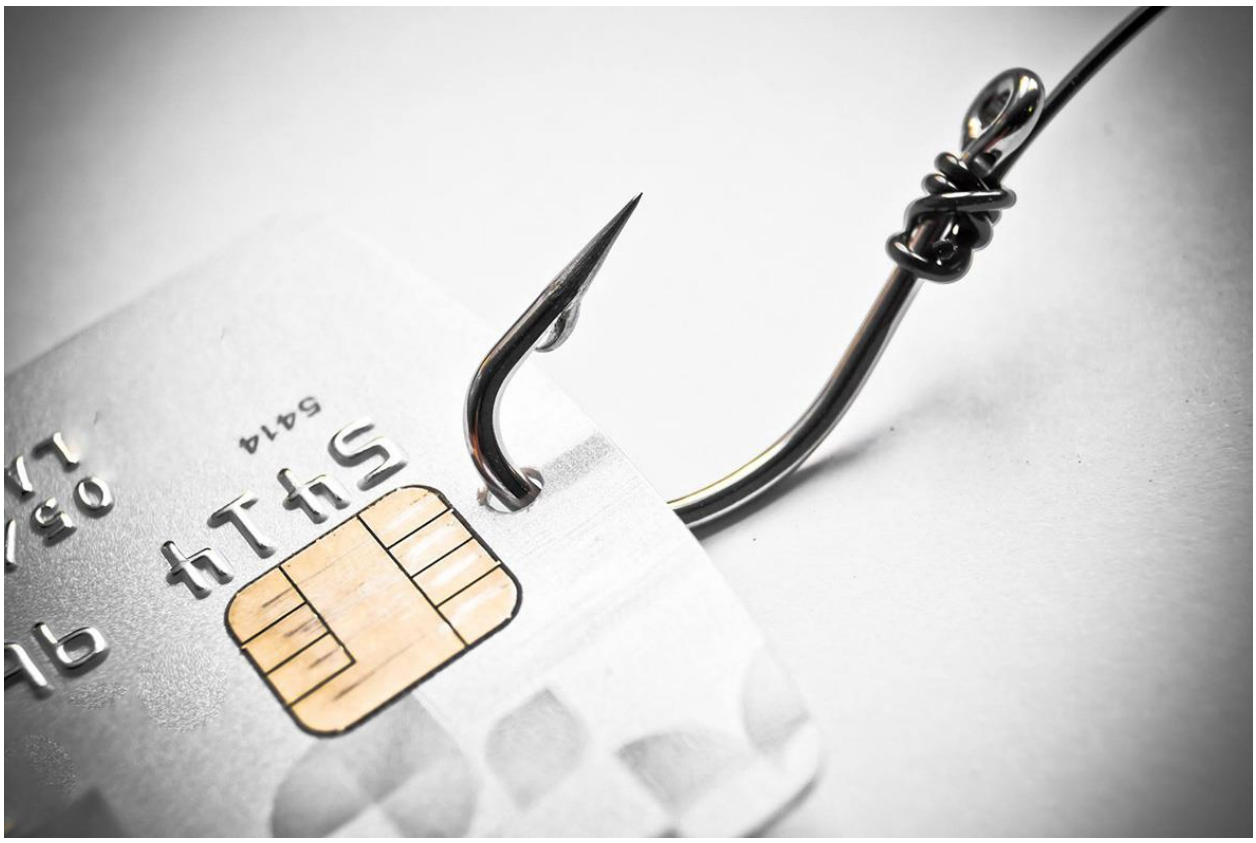
— В первую очередь, когда поступает звонок о том, что у человека пропали денежные средства, осуществляется несанкционированный доступ к его банковской карте, что может привести к потере средств, появляется чувство страха. В этом состоянии он готов идти по определенному алгоритму, который уже разработан злоумышленниками. Нет времени, возможности переключиться, подумать, оценить ситуацию. А на той стороне достаточно серьезная психологическая подготовка либо написаны специальные скрипты, программы, которые выстраивают определенный механизм вопросов, позволяющих не дать человеку опомниться, — рассказывает Алексей Новаш.

Атака на компании

Однако не только обычные граждане страдают от того, что их данные попали в общий доступ. Существенный вред наносится и компаниям. А с началом конфликта между Россией и Украиной активизировались киберпреступники.

Виртуальные аферисты собирают базу корпоративных почт, продают ее на теневых ресурсах. Покупатель организовывает массовую рассылку с одинаковым текстом сообщения и прикрепленным файлом. Если на него кликнуть, запускается опасный вирус. В итоге цифровая информация предприятия кодируется, и, по сути, фирма берется в заложники. Так произошло с одной минской компанией. Главный бухгалтер опрометчиво открыла пришедший на почту файл. Компьютер оказался зараженным. Потом киберворам удалось перевести около 50 тысяч рублей со счета организации на счет своего подельника.

Иногда хакеры взламывают почту компании и вклиниваются в деловую переписку. Недавно такой случай произошел в Клецком районе. Агропредприятие вело диалог с зарубежной фирмой о покупке техники. В итоге, когда дело дошло до перевода денег, 300 тысяч рублей ушли мошенникам.



Изучен мировой опыт

Почти два года назад вступил в силу Закон «О защите персональных данных». По словам заместителя председателя Постоянной комиссии Палаты представителей Национального собрания по национальной безопасности Игоря Мартынова, работу над правовым документом начали еще в 2018 году:

— В законе прописаны три категории персональных данных: общедоступные, специальные и иные. Особую защиту получили специальные. Они касаются расовой, национальной принадлежности, политических, религиозных взглядов, здоровья. Допустим, сведения о нашем здоровье в большинстве своем хранятся в медучреждениях. Человек, естественно, не желает, чтобы эта информация была разглашена. А если это происходит, предусмотрена ответственность в Уголовном, административном кодексах.

Помимо этого, в законе появились требования к сбору и использованию персональных данных.

— Хочу заметить, что люди стали осознаннее относиться к тому, кому и какую информацию они предоставляют. Например, во многих магазинах сейчас просят только номер телефона. И этого достаточно, чтобы стать участником дисконтной программы. А ведь номер телефона обезличен, это просто набор цифр.

Во время разработки законопроекта был изучен опыт ряда стран. И стоит отметить, что наш закон по сравнению с французским или немецким довольно мягкий, говорит Игорь Мартынов:

— Там ответственность за разглашение персональных данных гораздо выше, чем у нас. Доходит до лишения свободы на срок от десяти лет и более. У нас же подход более гуманный. Упор делается на сознание людей: одни должны быть более осмотрительны и осторожны, предоставляя сведения о себе куда-либо, другие — более ответственно следить за их сохранностью и должным образом наладить систему защиты.

Базы в общем доступе

В ноябре 2021 года в стране был создан Национальный центр защиты персональных данных. Он, в частности, является уполномоченным органом по защите прав субъектов персональных данных и осуществляет контроль за их обработкой. Причем как со стороны государственных, так и коммерческих структур.

Только в этом году произошло несколько крупных утечек. В сеть попали данные около миллиона клиентов двух торговых сетей. В обоих случаях причина — несанкционированный доступ к информационным системам.

Начальник управления контроля и аудита Национального центра защиты персональных данных Владимир Кузуро отмечает, что утечка сведений фиксируется довольно часто:

— Наши специалисты постоянно мониторят интернет, отслеживают по мере возможности базы, попадающие в общий доступ. И мы регулярно выявляем утечки.

Более 80% из них — хакерские атаки. Интересует злоумышленников в большинстве своем ретейл и те отрасли, где у компаний есть большое количество клиентов. Что касается сведений, которые попадают в чужие руки, — это фамилия, имя, отчество, номер телефона, адрес, электронная почта, логины, пароли…

— Человек, чьи персональные данные оказались в общем доступе, об этом иногда даже не подозревает и по этой причине очень уязвим для противоправных действий, — говорит Владимир Кузуро.

Наша информация порой становится оружием, которое мошенники направляют против нас. Помимо телефонных звонков, они могут

адаптировать фишинговое письмо под конкретного человека, что увеличит вероятность того, что жертва сделает все, что от нее требует мошенник.

— Сюда входят введение платежных данных на фишинговой странице, скачивание вредоносного файла, предоставление удаленного доступа, — перечисляет специалист.

В большом деле любая мелочь важна

К слову, организация не всегда знает, что у нее похищены некие сведения. Нередко об этом становится известно лишь от Национального центра защиты персональных данных. Если в сеть ушел большой инфомассив, назначается внеплановая проверка.

— Важная задача — проинформировать людей о том, что их данные в общем доступе. Это забота организации. То есть оператор должен любым способом сообщить всем клиентам, что произошла утечка. Помимо этого, около месяца на главной странице их сайта должен висеть баннер с сообщением о том, что данные клиентов утеряны. И призвать людей сменить логины, пароли и так далее. Затем организации необходимо перед нами отчитаться, прислать скриншоты того, что они выполнили все наши требования, — отмечает Владимир Кузуро.

Параллельно с этим центр проводит серьезную внутреннюю проверку, в ходе которой выясняется, почему стал возможен инцидент.

— Нарушения практически всегда связаны именно с нереализацией в полном объеме обязательных мер по обеспечению защиты персональных данных, предусмотренных статьей 17 Закона Республики Беларусь «О защите персональных данных», — говорит

Владимир Кузуро. — *У нас еще ни разу не было случая утечки в компании, где все требования по защите выполнены.*

Взломы — это в том числе и большие репутационные потери для предприятия. И чтобы восстановиться после этого, нужны годы.

— Сейчас мы видим, как крупные операторы меняют подходы к работе и понимают, чем больше данных они собрали, тем большую ответственность несут. Но есть и организации, которые уверены, что с ними ничего не произойдет: мол, маленькая компания, кому мы нужны. Исходя из практики, взламывают тех, у кого есть слабые места в системе, — уверен Владимир Кузуро.

Вместе с тем, если утечка произошла из-за невыполнения требований законодательства, есть еще и административная ответственность. Центр направляет материалы в органы внутренних дел, а оттуда они уже идут в суды. И организация, помимо всех потерь, вынуждена еще выплачивать штраф до 50 базовых величин. И это справедливо. Ведь оказавшиеся в свободном доступе сведения о человеке из сети уже убрать невозможно. При этом за незаконные действия в отношении информации о частной жизни и персональных данных, несоблюдение мер обеспечения защиты персональных данных также предусмотрена уголовная ответственность.

Кадрам уделяют первостепенное внимание

В организациях, на предприятиях сегодня в штате появляются сотрудники и даже подразделения, осуществляющие внутренний контроль за обработкой персональных данных.

— Важно понимать, что персональные данные — это ценный актив, который нуждается в такой же охране, как и материальные активы организации. Недостаточно внимательное отношение к этой работе может привести к несанкционированному доступу к информации, — подчеркивает начальник управления контроля и аудита Национального центра защиты персональных данных Владимир Кузуро. *— С сентября прошлого года наш центр проводит соответствующие курсы повышения квалификации. Их уже прошли почти 2,3 тысячи человек, более 2 тысяч обучались в рамках семинаров и вебинаров.*

Вместе с Институтом информационных технологий БГУИР ведется активная работа по открытию на базе университета новой специальности переподготовки кадров «защита персональных данных» на уровне высшего образования. Квалификация — «специалист по безопасности данных».

Всевидящее око

Камеры видеонаблюдения – еще один вопрос, над которым работает центр. Поступают жалобы от людей: мол, камеры устанавливают в рабочих кабинетах и местах общего пользования. А есть случаи, когда за людьми следят скрытно, не предупредив работников о камерах. В центре отметили, что разработали разъяснения для работодателей по этому вопросу. Помимо этого, совместно с Министерством ЖКХ, иными заинтересованными органами и организациями прорабатывается подход относительно видеонаблюдения в многоквартирных жилых домах. Эта работа будет продолжена.

FINANCEBUGG.COM

Не раз в сети люди жаловались, что с установленных в частном порядке в квартирах камер фото и видео вдруг оказывались на просторах интернета. Что необходимо делать, чтобы подобное не произошло с вами?

Во время подключения видеокамеры, советуют специалисты, нужно самостоятельно устанавливать пароль. Также следует убедиться, что мастер-установщик его не изменил. Еще одна опасность – хакерский взлом. Ведь, по сути, все технические устройства, подключенные к интернету, подвержены атакам. Однако если использовать сложный пароль, то такая ситуация маловероятна.

Что касается пароля, эксперты советуют включать в него, помимо букв и цифр, спецсимволы, например @, $, & и так далее. В интернете сейчас существует база самых популярных паролей, с которой тоже можно ознакомиться, чтобы не совершить ошибку. Нельзя устанавливать цифры, идущие подряд, дату рождения, клички домашних животных, все персональные данные, которые с вами связывают.

Какие поля заполнять?

Важно помнить о соблюдении требований по защите своих данных не только на работе, но еще и в быту. Например, когда приходим как клиенты в магазин и заполняем анкету, чтобы получить дисконтную карту, мы должны понимать, зачем о нас собирают столько информации. Заполнять следует только те поля, которые, как вы считаете, необходимы для достижения цели. Если вы хотите стать участником программы лояльности, то надо дать реквизиты, как с вами связаться. Паспортные данные, сведения о родственниках не нужны. Или же для того чтобы вас идентифицировать, необходимо лишь предоставить свою фамилию и имя.

Биометрия несовершеннолетних

Ранее в Национальном центре защиты персональных данных было заявлено, что будет вестись работа по упорядочению обработки данных несовершеннолетних. Особенно биометрических. Ведь их утечка может иметь серьезные последствия для ребенка, отмечает Владимир Кузуро:

— *В большей степени обработкой таких данных занимаются учреждения образования и здравоохранения. Центр во взаимодействии с профильными министерствами проводит активную разъяснительную работу с учреждениями образования и здравоохранения по применению закона о защите персональных данных. То есть обрабатывать биометрические данные детей теперь можно будет только в случаях, которые предусмотрены законодательными актами и в минимально необходимом объеме.*

yankovich@sb.by

Александра ЯНКОВИЧ