По статистике Банка России, за I квартал 2021 года через системы дистанционного банковского обслуживания (ДБО) – интернет-банк и личные кабинеты – похищено более 1 млрд рублей. Это почти в 2 раза больше, чем за тот же период прошлого года. Об этом шла речь на встрече с предпринимателями Тюмени по вопросам информационной безопасности в условиях цифровизации бизнеса.

Мероприятие состоялось 29 июля по инициативе ТРО ООО «Деловая Россия». Представители регионального отделения Банка России и Ассоциации кредитных организаций Тюменской области рассказали об основных киберугрозах для бизнеса, фишинговых рассылках, дали рекомендации, как защититься от дистанционных краж и финансовых мошенников.

Цифровые технологии, дистанционное получение товаров и услуг прочно вошли в жизнь россиян с началом пандемии. Большинство организаций, в том числе в финансовой сфере, переориентировались на работу в удаленном режиме, что позволило преступникам внедрить новые схемы. В прошлом и в начале этого года Банк России зафиксировал значительный рост количества фишинговых рассылок, а также мобильного мошенничества.

По словам заместителя начальника отдела безопасности Отделения Банка России по Тюменской области Алексея Нохрина, в системах ДБО юридических лиц в целом по России в I квартале 2021 года выявлено более 1,5 тыс. операций без согласия клиента, что на 60% больше, чем год назад. Ущерб компаний превысил 560 млн рублей, а доля социальной инженерии, т.е. метода получения доступа к конфиденциальным данным с использованием психологического воздействия, возросла с 44% до 80%. Сценарии могут быть различными. Мошенники втягивают клиента в разговор, входят в доверие, торопят и выманивают данные карты или пароль от личного кабинета. Причем вернуть эти деньги совсем не просто, ведь человек сам сообщил персональные данные мошенникам. По этой причине банки вернули лишь 1% похищенных средств компаний. Банк России рекомендовал кредитным организациям активнее информировать своих клиентов о рисках мошенничества и правилах кибербезопасности.

Вице-президент Ассоциации кредитных организаций Тюменской области Александр Расковалов сообщил, что ***выявляются единичные случаи проникновения к счетам клиентов-юридических лиц*** . Кибермошенники регистрируют доменные имена, схожие по написанию с доменами известных компаний; для этих

доменов создаются почтовые серверы, с которых производятся фишинговые рассылки. Мошеннические письма содержат вложения, запускающее модуль, который ищет на компьютере жертвы систему ДБО. После этого загружается и незаметно устанавливается программа для удаленного управления зараженным компьютером, в системе ДБО создаются платежные поручения и отправляются в банк, который переводит средства на счета преступников.

Спикер подчеркнул, что всплеск утечки корпоративной информации также связан с переводом части сотрудников в период пандемии на режим удаленной работы. Электронная почта по-прежнему остается одним из основных векторов атак. Злоумышленники адресно атакуют переведенных на дом сотрудников, заражая их компьютеры вредоносными программами, и затем получают доступ в корпоративную сеть.

Специалисты отметили, что защитить денежные средства от внешних угроз можно только в тесном взаимодействии кредитных организаций и клиентов. Банки направляют огромные суммы и усилия для разработки программного обеспечения, противодействующего взломам, утечкам данных, хищений средств, но подавляющее большинство инцидентов реализуется на стороне клиента. Поэтому важной задачей является вовлеченность клиентов в процесс информационной безопасности – осознание и понимание необходимости защиты своих активов, обеспечение организационных мероприятий и внедрение технических средств защиты. Для минимизации киберрисков компаниям следует уделять повышенное внимание цифровой гигиене, проводить учения своих сотрудников, которые будут включать в себя грамотную работу в сети Интернет, с электронной почтой, личными кабинетами и паролями.

29 июля 2021 года