CYBER READINESS
INSTITUTE

Новая причина для страха Период подачи налоговой декларации: кибератаки

Срок подачи налоговой декларации стремительно приближается. Вы просматриваете бумаги, разложенные на столе, пытаясь найти пропавшую налоговую форму. Всю последнюю неделю вы получаете постоянный поток электронных писем от вашего бухгалтера с просьбами предоставить недостающую информацию. Ему нужна такая-то форма, такая-то квитанция; ему нужно, чтобы вы классифицировали расходы. Вы расстраиваетесь и отвлекаетесь.

Еще одно электронное письмо приходит от вашего бухгалтера. Он просит вас нажать на ссылку и указать свой номер социального страхования. Вы прекращаете рыться в бумагах и рефлекторно нажимаете на ссылку.

Но, опомнившись, вы останавливаетесь. «Моя бухгалтерская фирма знает мой номер социального страхования. Они заплатили мои налоги в прошлом году». Поэтому вместо того, чтобы нажать на ссылку, вы начинаете отвечать на письмо, но затем до вас доходит. «Если это фишинговое письмо, и если я отвечу, оно вернется к хакерам».

Вы принимаете мудрое решение позвонить в свою бухгалтерскую фирму. Они отчаянно говорят вам, что их взломали, и одно и то же фишинговое письмо было отправлено всем их клиентам. Они не могут использовать электронную почту, чтобы предупредить своих клиентов, поэтому звонят им по одному и молятся, чтобы никто не нажал на ссылку.

В бухгалтерской фирме полный хаос. В период подачи налоговой декларации все всегда безумно загружены, но кибератака добила их окончательно. Мало того, что их электронная почта была скомпрометирована, хакеры требуют выкуп, чтобы разблокировать все данные их клиентов.

Когда началась атака, никто не знал, что делать. Они никогда даже не слышали о плане реагирования на киберинциденты. Фирма лихорадочно позвонила своему ИТ-консультанту, который спросил ее, есть ли у них текущие резервные копии клиентских данных. «Мы думали, их делаете вы!» — кричали они ИТ-консультанту. «Нет. Это ваша ответственность», — прозвучал спокойный ответ.

Консультант по информационным технологиям сказал, что все ПО было обновлено, поэтому хакеры, вероятно, проникли в систему бухгалтерской фирмы через слабые пароли, или кто-то перешел по ссылке.

Бухгалтерская фирма начала звонить своим клиентам, чтобы сообщить им о поддельном электронном письме с запросом предоставить номер социального обеспечения. Фирма должна была предупредить каждого клиента о том, что их личная информация может быть скомпрометирована, и объяснить, что им нужно будет попросить отсрочку для подачи налоговой декларации. Двадцать лет создания надежной клиентской базы оказались под угрозой в один ужасный день. Партнеры пообещали принять меры по киберготовности, следуя приведенным ниже советам.

guide@cyberreadinessinstitute.com

6 важных советов по кибербезопасности в период подачи налоговой декларации

Консультации для физических лиц и налоговых органов

Используйте надежные пароли: убедитесь, что вы используете парольные фразы из 15 или более символов для своих программ и уникальные парольные фразы для своих учетных записей. Включите многофакторную аутентификацию в своих учетных записях, когда это возможно.

Обновление программного обеспечения: включите автоматическое обновление и убедитесь, что исправления вашего программного обеспечения установлены, особенно каждый год перед периодом подачи налоговой декларации. Учитывая, сколько работы проводится в Интернете в этот период, все уязвимы.

Безопасный обмен файлами: никогда не сообщайте и не запрашивайте номер социального страхования или любые другие конфиденциальные финансовые данные по электронной почте или через Интернет. Подтверждайте любую запрошенную финансовую сделку (например, банковский перевод, прямой депозит) или запрос личной информации с помощью телефонного звонка лицу, которое ее запрашивает. Убедитесь, что ваш обмен файлами/онлайн-портал защищен и зашифрован.

Резервное копирование и тестирование: регулярно делайте резервные копии важных данных и проверяйте свои резервные копии каждый месяц.

Имейте план: убедитесь, что у вас есть проверенный план реагирования на инциденты для вашей организации. В случае нарушения важно иметь план реагирования и восстановления, который можно активировать немедленно. Общение между вами и вашими клиентами также имеет решающее значение в случае неавторизированного доступа.

Будьте осторожны: вы уже знаете, что IRS никогда не будет связываться с физическими лицами по телефону или электронной почте. Но будьте осторожны с электронными письмами от вашего налогового агента. Если что-то выглядит не так, не открывайте письмо, пока не позвоните, чтобы убедиться, что оно законно. Это популярное время года, когда кибермошенники пытаются обманом заставить людей отправить личную финансовую информацию.

Об Институте киберготовности

Институт киберготовности - это некоммерческая инициатива, объединяющая лидеров бизнеса из разных секторов и географических регионов с целью обмена ресурсами и знаниями,, которые используются для разработки бесплатных инструментов кибербезопасности в малых и средних предприятиях (МСП). Изучите основы хорошей кибербезопасности с помощью нашего Стартового набора или создайте культуру киберготовности в своей организации с помощью самостоятельной онлайн-программы киберготовности. В наших руководствах по ресурсам для удаленной работы и гибридным рабочим местам вы найдете своевременные советы по решению современных киберпроблем. Чтобы узнать больше посетите сайт **www.BeCyberReady.com.**