CYBER READINESS
INSTITUTE

Um novo motivo para temer a temporada de impostos: Ataques de cibersegurança

O prazo para a apresentação de impostos está a aproximar-se rapidamente. Está à procura dos papéis espalhados pela mesa da sala de jantar, tentando encontrar o formulário de imposto que está a faltar. Na semana passada, recebeu um fluxo constante de e-mails do seu contabilista pedindo informações que faltavam. Eles precisam deste formulário; eles precisam daquele recibo; eles precisam de si para categorizar uma despesa. Está a ficar frustrado e a distrair-se.

Chegou outro e-mail do seu contabilista. Neste está a pedir que clique numa ligação e forneça o seu número de segurança social. Para de procurar pelos papéis e, por reflexo, começa a clicar na ligação.

Mas algo vem-lhe à cabeça e para. “A empresa de contabilidade sabe o meu número de segurança social. Eles ficaram encarregados dos meus impostos no ano passado.” Então, em vez de clicar na ligação começa a responder ao e-mail, mas aí percebe. “Se for um e-mail de phishing e eu responder, ele irá voltar para os hackers.”

Sabiamente decide pegar no telefone e ligar para a sua empresa de contabilidade. Informam que foram hackeados e que o mesmo e-mail de phishing foi enviado para todos os clientes. Não podem usar o e-mail para avisar os clientes. Então, têm telefonado para cada um deles e rezado para ninguém clique na ligação.

Na empresa de contabilidade, é o caos total. A temporada de impostos é sempre extremamente agitada, mas o ataque cibernético está a levá-los ao limite. Não só o seu e-mail foi comprometido, mas os hackers estão a exigir dinheiro para desbloquear todos os dados dos seus clientes.

Quando o ataque começou, ninguém sabia o que fazer. Eles nunca tinham ouvido falar de um plano de resposta a incidentes cibernéticos. Eles ligaram freneticamente para o consultor de TI, que perguntou se eles tinham cópias de segurança atualizadas dos dados dos clientes. "Pensei que estava a tratar disso!" gritaram eles com o consultor de TI. “Não. Essa é a vossa responsabilidade”, foi a resposta calma.

O consultor de TI disse que todo o software estava atualizado, então os hackers provavelmente entraram no sistema da empresa de contabilidade através de palavras-passe fracas ou quando alguém clicou numa ligação.

A empresa de contabilidade começou a ligar para os seus clientes para informá-los sobre o e-mail falso. Tiveram que avisar cada cliente que as suas informações pessoais poderiam estar comprometidas e explicar que eles precisariam de mais algum tempo para tratarem dos impostos. Vinte anos a construírem uma base de clientes confiável que foi colocada em risco num dia horrível. Os parceiros prometeram ficar preparados para ataques cibernéticos seguindo os conselhos abaixo.

6 dicas essenciais de cibersegurança para a temporada de impostos

Conselhos para indivíduos e contabilistas

Use palavras-passe fortes: Certifique-se de de que usa uma frase de acesso com 15 carateres ou mais para os seus programas e de usar frases de acesso exclusivas nas suas contas. Ative a autenticação multifator nas suas contas, sempre que possível.

Atualize o software: Permita a atualização automática e garanta que os seus patches de software são instalados, especialmente antes da temporada de impostos a cada ano. Considerando quantos negócios são conduzidos online durante a temporada de impostos, todos estão vulneráveis.

Troca de ficheiros segura: Nunca forneça ou peça um NISS - ou quaisquer outros dados financeiros confidenciais - por e-mail ou online. Valide qualquer transação financeira solicitada (por exemplo, transferência eletrónica, depósito direto) ou solicitação de informações pessoais com um telefonema para o indivíduo que está a solicitar tal operação. Certifique-se de que a troca de ficheiros é segura e encriptada.

Cópias de segurança e teste: Crie cópias de seguranças dos seus dados críticos regularmente e teste as suas cópias de seguranças todos os meses.

Tenha um plano: Certifique-se de que tem um plano de resposta a incidentes. No caso de ocorrer uma violação, é fundamental ter um plano de resposta e recuperação que possa ativar imediatamente. A comunicação entre si e os seus clientes também é crítica em caso de violação.

Tenha cuidado: Já sabe que o departamento de finanças nunca entrará em contacto com pessoas por telefone ou e-mail. Mas tenha cuidado com os e-mails do seu contabilista. Se algo não estiver certo, não abra o e-mail antes de ligar para verificar se é legítimo. Esta é uma época popular do ano, em que os cibercriminosos tentam enganar as pessoas para que enviem informações financeiras pessoais.

Sobre o CRI

O Cyber Readiness Institute é uma iniciativa sem fins lucrativos que reúne líderes empresariais de vários setores e regiões geográficas para a partilha de recursos e conhecimento que informam o desenvolvimento de ferramentas gratuitas de segurança cibernética para pequenas e médias empresas (PMEs). Explore os blocos de construção de uma boa segurança cibernética com o nosso Kit de Iniciação ou crie uma cultura de prontidão cibernética na sua empresa com o programa de prontidão cibernética online. Os nossos recursos de trabalho remoto e guias de local de trabalho híbrido oferecem dicas oportunas para lidar com os desafios cibernéticos em evolução nos dias de hoje. Para saber mais, visite www.BeCyberReady.com.