Fraude Através de Pirataria de Email Profissional (Business Email Compromise)

Um alerta de segurança do fornecedor.

A MSD leva a sério a fraude e a proteção da informação.

Saiba que, com a nossa crescente dependência da comunicação virtual, a incidência dos casos de pirataria em Emails profissionais (Business Email Compromise (BEC)) está a aumentar. A pirataria em Emails profissionais utiliza o email e outras comunicações eletrónicas para se fazer passar por um executivo, funcionário ou outra pessoa de autoridade.
Os pedidos de pagamentos ou de acesso à folha de pagamentos dos funcionários ou à informação W2 (apenas EUA) são então realizados de forma fraudulenta em nome de uma empresa.

O que deve saber
A MSD está empenhada em proteger o seu negócio e as suas informações bancárias. De acordo com o nosso

Gabinete de Privacidade Global, os nossos processos e diretrizes de Tecnologia de Informação, e alinhados com os regulamentos locais e regionais, o nosso pessoal formado aplica processos e controlos rigorosos na recolha, validação e captura de dados, com múltiplos pontos de verificação e auditorias regulares sobre os nossos procedimentos e práticas.

Para melhor proteger o seu negócio:

- Utilize canais secundários, ou autenticação de dois fatores, para verificar independentemente os pedidos de alteração de informações de conta.
- Assegure-se de que os URLs nos e-mails estão associados à empresa de onde dizem ser.
- Esteja atento a hiperligações que contenham erros de ortografia do nome de domínio real.
- Verifique o endereço de email utilizado para enviar emails, comparando-o com o remetente, especialmente quando utilizar um dispositivo móvel ou portátil.
- Crie filtros de sistema de deteção de intrusão para sinalizar emails com extensões que se assemelham a emails da empresa Por exemplo, o email legítimo de ceo@abc_company.com sinalizaria como email fraudulento o email de ceo@abc-company.com.
- Monitorize as contas financeiras regularmente para detetar irregularidades, tais como depósitos em falta.
- Mantenha atualizados todos os patches de software e todos os sistemas.
- Assegure-se de que as definições nos computadores dos funcionários permitem a visualização das extensões completas de email.
- Conheça as informações de contacto do seu Centro de Resolução local, alertando-os se se sentir vítima de pirataria nos Emails profissionais e se esta estiver relacionada com a Merck ou MSD; caso contrário, contacte as autoridades policiais locais.

A Merck é conhecida como MSD fora dos Estados Unidos e do Canadá.