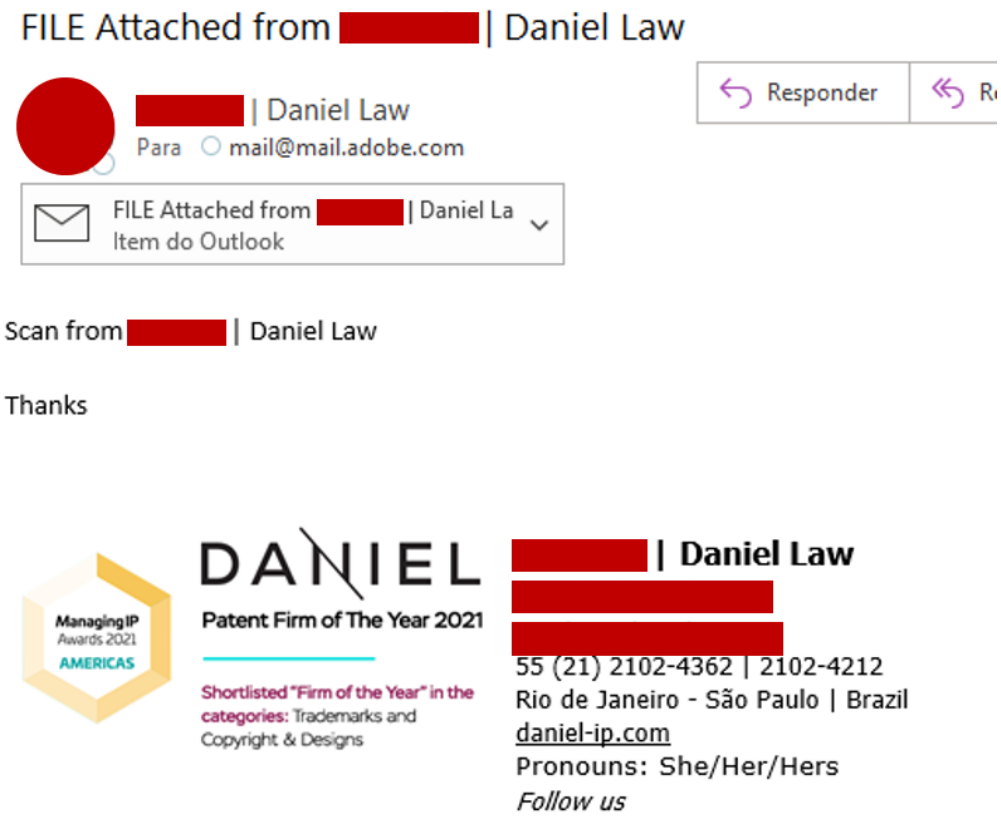
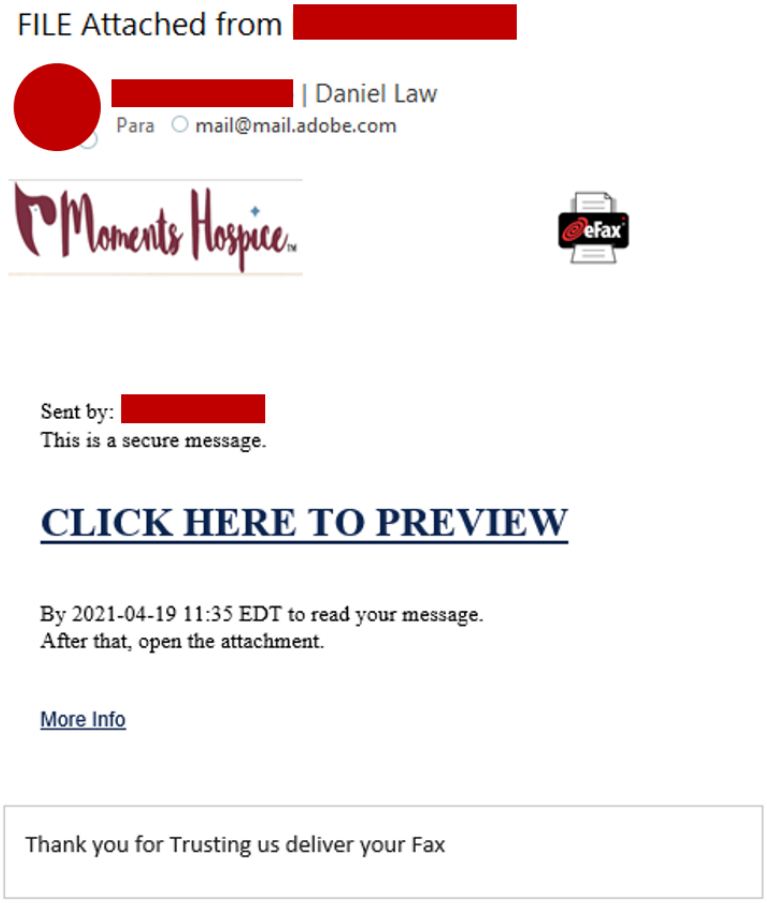
20 de abril de 2021

E-mails estranhos, mesmo de um remetente confiável, podem ser conteúdo malicioso

Recentemente, muitas pessoas do escritório receberam um e-mail malicioso partindo do e-mail de um colaborador.





Trata-se de uma tentativa de ataque embarcado em um site de notícias. No momento em que o colaborador leu a informação, "pipocou um site mal-intencionado" em sua tela e, apesar de tentar fechar o conteúdo, o malware (código malicioso) já estava instalado.

Os efeitos dessa tentativa de invasão foi o envio de e-mails para parte dos sócios e colaboradores da Daniel. A TI já solucionou a questão e recomenda que ninguém abra os "e-mails estranhos" recebidos, ainda que eles sejam de um remetente confiável.

Casos como esse servem de reforço para tomarmos cuidado com o tipo de conteúdo que acessamos. Os bloqueios nos equipamentos da Daniel existem justamente para prevenir conteúdos que, mesmo não intencionalmente, contenham um malware.

Precisamos redobrar a atenção para que nossos equipamentos fiquem seguros:

1. Trabalhar conectado a VPN, para que assim o antivírus corporativo esteja sempre automaticamente atualizado, protegendo assim nossos equipamentos;
2. Verificar e tomar cuidado com todo e qualquer conteúdo que seja acessado em todos os nossos dispositivos. Evitando entrar em sites pouco confiáveis ou com informações duvidosas, tendenciosas ou mesmo fake news;
3. Prestar atenção aos conteúdos "estranhos" recebidos, ainda que eles sejam encaminhados de contados confiáveis. Nunca se sabe quando a pessoa pode ter sido alvo de um ataque de um vírus ou outro malware.

Seguindo essas recomendações, conseguiremos manter os nossos equipamentos, e o dos nossos colegas e familiares, mais seguros.