



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.

FILE Attached from [REDACTED] | Daniel Law



[REDACTED] | Daniel Law
Para mail@mail.adobe.com

↳ Responder

↳ Reply



FILE Attached from [REDACTED] | Daniel La
Item do Outlook

Scan from [REDACTED] | Daniel Law

Thanks



DANIEL

Patent Firm of The Year 2021

Shortlisted "Firm of the Year" in the categories: Trademarks and Copyright & Designs

[REDACTED] | Daniel Law


[REDACTED]
[REDACTED]

55 (21) 2102-4362 | 2102-4212
Rio de Janeiro - São Paulo | Brazil
daniel-ip.com

Pronouns: She/Her/Hers

Follow us

FILE Attached from [REDACTED]

 [REDACTED] | Daniel Law
Para  mail@mail.adobe.com



Sent by: [REDACTED]
This is a secure message.

[CLICK HERE TO PREVIEW](#)

By 2021-04-19 11:35 EDT to read your message.
After that, open the attachment.

[More Info](#)

Thank you for Trusting us deliver your Fax

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 contatos 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.

