Orientações para se proteger contra fraudes de phishing

- De acordo com as políticas de finanças e controle do Grupo Sidel, a Sidel opera um sistema de autorização dupla, incluindo quaisquer alterações de instrução de pagamento. Estas alterações devem ser aprovadas previamente, por escrito, por duas pessoas autorizadas por uma entidade legal da Sidel. Tais mudanças de instrução de pagamento são extremamente raras. A Sidel raramente solicita que o pagamento seja alterado de um banco para outro, especialmente para um país terceiro.
- Para todos os pedidos de pagamento, uma fatura da Sidel sempre é anexada. Portanto, você deve suspeitar imediatamente de tais pedidos que não contenham uma fatura correta.
- Para todos os lembretes ou consultas de acompanhamento relativas a pagamentos, uma referência ao pedido original e sua fatura é sistematicamente incluída. Portanto, você deve suspeitar imediatamente de qualquer pedido que não contenha uma referência correspondente ao pedido inicial e à fatura.
- Em caso de quaisquer alterações aos seus pedidos de pagamento normais e instrução de pagamento de agentes ou entidades jurídicas da Sidel, (mesmo que Sidel pareça ser o remetente), recomendamos sempre confirmar verbalmente as instruções através de uma chamada telefônica para o seu contato de confiança na Sidel, usando o seu número habitual de contato com a Sidel. **Não** utilize os dados de contato fornecidos pelo remetente que aparecem em pedidos de pagamento e mudanças de instruções de pagamento. Em vez disso, ligue para o seu contato de confiança na Sidel usando seu número habitual de contato com a Sidel. Isto é especialmente importante caso você receba um pedido de transferência de fundos ou solicitação de informações confidenciais de negócios a partir de um endereço de e-mail que pareça diferente do formato nome.sobrenome@sidel.com.
- A Sidel só se comunica a partir de um endereço de e-mail sidel.com, como nome.sobrenome@sidel.com. A Sidel não utiliza qualquer outro endereço de e-mail terminando com sidel.net, side1.com, sidei.com etc.
- Não abra, nem responda e-mails spam de terceiros.
- Não responda a chamadas telefônicas ou mensagens de e-mail pedindo informações comerciais confidenciais ou pessoais. Sempre verifique a fonte (através do registro dos detalhes do pedido inicial e, em seguida, retornando a chamada telefônica para a pessoa nomeada através de um número de contato verificado).
- Ao enviar informações confidenciais de negócios por e-mail, considere a possibilidade de criptografar a mensagem.
- Ao acessar sites usando mecanismos de busca populares, verifique se o site que você está contatando é legítimo, verificando o endereço URL que muitas vezes é apresentado pelo mecanismo de busca.
- Sempre verifique a identidade de qualquer pessoa com quem se comunica por forma eletrônica (como e-mail) e o propósito do seu pedido se você estiver desconfiado.
- Sempre desconfie de mensagens externas de e-mail contendo links para acessar sites, não importa o quão legítima a mensagem de e-mail possa parecer.

- Nunca clique em um hiperlink (como um link para uma página da Internet) em um e-mail se você estiver desconfiado da mensagem ou do remetente. Se você for direcionado para o site da Sidel a partir de um e-mail, verifique sempre se o endereço do site é um endereço válido sidel.com.
- Os principais sites que a Sidel utiliza para comunicações externas são www.sidel.com, www.sidel.de, www.sidel.pt, www.sidel.es, www.sidel.cn, www.sidel.fr e www.sidel.ru . Caso lhe seja solicitado em um e-mail acessar outro site da Sidel, não acesse o link. Em vez disso, verifique primeiro através de uma chamada telefônica com o seu respectivo contato na Sidel.
- Sempre atualize os computadores com os patches de segurança mais recentes. Os sistemas operacionais (como o Windows) são regularmente aprimorados por seus fornecedores, que oferecem melhorias de segurança. O Windows, por exemplo, permite que os usuários instalem automaticamente as atualizações de segurança através do site http://windowsupdate.microsoft.com.
- Os navegadores de Internet (como o Internet Explorer, Mozilla Firefox, Google Chrome, Safari (Apple), etc.) já oferecem proteção contra sites fraudulentos e têm funcionalidades anti-phishing em seus menus. O(s) seu(s) navegador(es) também deve(m) ser regularmente atualizado(s) com a versão mais recente.
- Todo o software em computadores deve ser atualizado regularmente. Os fornecedores regularmente enviam mensagens pop-up para propor uma atualização do seu software.
- Considere a possibilidade de instalar antivírus e software anti-spyware (que muitas vezes estão disponíveis no mesmo produto) e certifique-se que sejam a versão mais recente. Este tipo de software também deve ser atualizado regularmente.
- A maioria dos softwares antivírus depende de uma base de dados de vírus, que pode ser atualizada até mesmo várias vezes ao dia. O software antivírus pode ser configurado para instalar automaticamente as atualizações do banco de dados para garantir a máxima proteção. Você pode executar a varredura no seu computador depois que o antivírus for instalado ou atualizado para verificar se há qualquer possível infecção.
- Considere a possibilidade de ativar um firewall pessoal. Isso permite que você proteja o computador contra invasões e controle o tráfego de entrada e de saída.
- Proteja o seu e-mail. O seu software de e-mail deve ser equipado com um filtro anti-spam. O acesso ao e-mail deve ser protegido com login e uma senha forte.
- Se houver qualquer suspeita de que o seu endereço de e-mail tenha sido alvo de hackers, considere a possibilidade de usar um novo endereço de e-mail, e comunique devidamente esta mudança a todos os seus contatos de negócios.

Por último, lembre-se de sempre verificar cuidadosamente quaisquer pedidos de alteração no envio de recursos e/ou de dados bancários, e verificar a identidade do remetente autorizado. Confirme o pedido com uma chamada para o remetente utilizando seus dados de contato normais (ou seja, não use os dados de contato fornecidos no e-mail).

Mais informações, incluindo conselhos e orientações, podem ser encontradas nos sites internacionais de apoio http://www.stopthinkconnect.org/ e http://www.antiphishing.org/.