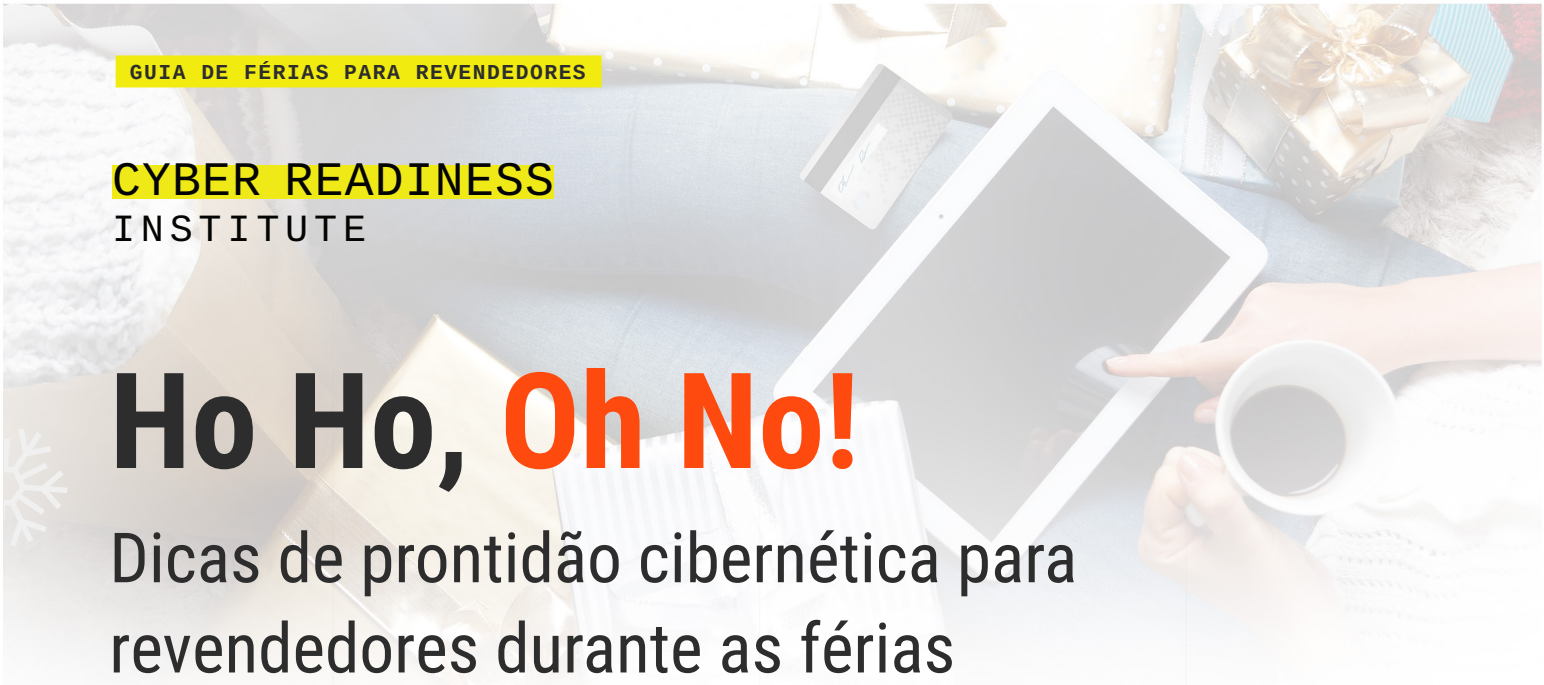
CYBER READINESS
INSTITUTE



Ho Ho, Oh No!

Dicas de prontidão cibernética para revendedores durante as férias

A temporada de compras natalícias está a chegar a todo vapor, mas, como tantas atividades regulares, **as compras estão diferentes este ano por causa da pandemia COVID-19.**

Mais pessoas estão a realizar compras online. De acordo com a McKinsey, entre 30 e 60 por cento dos consumidores em todo o mundo esperam fazer as suas compras online durante as férias. Os revendedores tiveram que reagir tornando mais fácil para os consumidores comprarem online e estabelecer novas maneiras de os compradores receberem as suas compras. Para muitos revendedores, essa realidade tem levado à contratação de serviços de entrega, o que significa que os revendedores estão a partilhar informações dos clientes com terceiros. Todo o processo de compra, do início ao fim, depende cada vez mais da transferência de informações entre si e os seus clientes, que usam computadores e smartphones. A tecnologia avançada de hoje possibilitou que os revendedores - mesmo os pequenos - transferissem rapidamente mais dos seus negócios para uma plataforma digital. Essa é uma ótima notícia para lidar com os desafios comerciais que aumentaram por causa da pandemia.

A má notícia é que os criminosos também migraram para o mundo digital. Os cibercriminosos sabem que mais pessoas estão a realizar compras online e que os revendedores estão a recolher e a partilhar informações mais valiosas sobre os seus clientes - incluindo números de cartão de crédito, endereços e identificação com foto. Houve um aumento enorme nos ataques de phishing de e-mail e texto - tentativas de fazer com que o utilizador clique num link ou envie informações - e ataques de ransomware em que criminosos mantêm o seu sistema de computador e dados como reféns até receberem um pagamento. O FBI relatou um aumento de 400 % nas reclamações de ataques cibernéticos anteriores à COVID-19. Enquanto a Interpol rastreou uma “taxa alarmante de ataques cibernéticos” dirigidos a empresas de todos os tamanhos, governos e infraestrutura crítica durante a pandemia.

Sabemos que é uma época agitada do ano e que está focado em atender os seus clientes. Percebemos que pode recrutar trabalhadores sazonais ou começar a trabalhar com novos serviços de entrega e parceiros. Mas os criminosos também sabem disso e esperam que se distraia e negligencie a prontidão cibernética. Infelizmente, 60 % das pequenas empresas fecham as portas em 6 meses após um grave incidente cibernético, de acordo com a National Cyber Security Alliance.

guide@cyberreadinessinstitute.com

Pode pensar que a sua empresa é muito pequena para ser um alvo, mas pode ser uma porta de entrada fácil para um alvo maior desejado.
Aqui estão algumas dicas para ajudá-lo a estar preparado para um ataque cibernético na temporada de compras de Natal:

A fazer

- Atualize imediatamente as suas palavras-passe para 15 caracteres - usar uma frase de acesso pode torná-la mais fácil de lembrar (por exemplo, letra de uma música, linha de um livro)
- Ative as atualizações automáticas para todos os softwares
- Use a autenticação multifator sempre que estiver disponível
- Certifique-se de que os seus computadores e dados têm uma cópia de segurança numa rede separada e teste essa cópia de segurança regularmente
- Tenha políticas cibernéticas claras e comunicadas a todos os funcionários
- Dê formação aos funcionários sobre como receber e processar pedidos online de forma segura

A não fazer

- Não clique em ligações e nunca forneça informações financeiras por e-mail
- Não partilhe as suas palavras-passe ou credenciais de início de sessão
- Não deixe nenhum computador sem supervisão e/ou desbloqueado
- Não presuma que os seus terceiros estão prontos para um ataque cibernético (por exemplo, serviços de entrega, processadores de pagamento, pequenos fornecedores)

Lembre-se de que o comportamento humano é fundamental para prevenir um ataque cibernético.

Certifique-se de que todos os seus funcionários e trabalhadores sazonais recebem formação quanto a políticas de segurança cibernética, que conheçam a importância da segurança cibernética e o seu papel. Ajude-os a desenvolver bons hábitos de prontidão cibernética. Para obter mais detalhes, inscreva-se no programa de prontidão cibernética e consulte os nossos **outros guias** para desenvolver bons hábitos de prontidão cibernética.

Sobre o Cyber Readiness Institute

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**.

guide@cyberreadinessinstitute.com