



CHOLTICHA_KRANJUMNONG_CANVA

UMA DAS DATAS MAIS IMPORTANTES

DIA DAS MÃES: UMA DATA LUCRATIVA PARA O VAREJO E UM CAMPO FÉRTIL PARA CIBERCRIMES

O Dia das Mães é uma das datas mais importantes para o varejo brasileiro, movimentando milhões em vendas todos os anos. De acordo com um estudo da Rakuten Advertising, em 2023 o Dia das Mães teve um aumento do ticket médio de 25% nas vendas online em relação ao ano anterior, e a tendência é que em 2024 não seja diferente.

Thiago Bertacchini (*)

Segundo uma recente pesquisa publicada pela Opinion Box, cerca de 77% dos brasileiros pretendem presentear alguém no segundo domingo de maio. No entanto, junto com o aumento das transações comerciais, também vem o risco crescente de atividades fraudulentas.

Com o avanço da tecnologia, os criminosos encontraram novas maneiras de explorar pontos fracos nas empresas, especialmente durante períodos de alta demanda como este. O mercado brasileiro tem sido palco de uma rápida inovação tecnológica, trazendo consigo o desafio de estarmos diariamente um passo à frente dos fraudadores.

Empresas que buscam se destacar precisam se adaptar rapidamente às novas e mais variadas táticas de fraude, como a criação de páginas falsas na web que se assemelham muito aos sites legítimos de e-commerces conhecidos ou até fraudadores que enviam e-mails em massa, mensagens de texto ou mensagens pelo WhatsApp oferecendo promoções tentadoras, como descontos exclusivos ou produtos gratuitos.

Diante disso, a integração de soluções de segurança eficazes sem comprometer a experiência do usuário tornou-se uma prioridade. E, para combater as ameaças crescentes, o uso de inteligência artificial (IA) e machine learning é uma estratégia crucial. Essas tecnologias não apenas identificam padrões complexos de atividade suspeita, mas também se adaptam continuamente para acompanhar a evolução das fraudes. Além disso, a autenticação multifatorial tem se mostrado eficaz na proteção contra acessos não autorizados.

Durante períodos de pico de vendas, os fraudadores se aproveitam da distração e da pressa dos consumidores e lojistas para realizar ataques cibernéticos. Por isso, as empresas podem adotar uma série de medidas para pro-



Mikael_Bromvriel_de_Pexels_CANVA

teger seus sistemas e dados durante o Dia das Mães e em qualquer outro momento do ano. Isso inclui:

Implementação de Autenticação Multifatorial (MFA), que adiciona uma camada extra de segurança exigindo múltiplas formas de verificação de identidade. Além de solicitar senha, as empresas devem implementar métodos como códigos de verificação enviados por SMS, autenticação por aplicativo móvel ou tokens de segurança.

Monitoramento de transações suspeitas em tempo real, que utiliza ferramentas de análise de dados para identificar padrões suspeitos de atividade, como transações incomuns, como compras de alto valor ou múltiplas tentativas de login fracassadas;

Auditoria de segurança regular identificar e corrigir vulnerabilidades nos sistemas e infraestrutura de TI, como testes de penetração, análise de código fonte e avaliações de risco, e aprimoramento de políticas de privacidade e segurança de dados, revisando e atualizando-as regularmente para garantir conformidade com regulamentações, como a Lei Geral de Proteção de Dados (LGPD).

Além das medidas mencionadas acima, é importante que empresas que realizem vendas online estejam constantemente - isto é, além dos períodos de picos de vendas - atentas a estratégias que vão fortalecer sua cibersegurança durante todo o ano, como:

- A utilização de firewalls e antivírus, que são a primeira linha de defesa contra ataques cibernéticos. Eles ajudam a bloquear ameaças externas e a identificar malware que pode comprometer os sistemas da empresa;
- Certificar-se de que mantém sistemas operacionais, aplicativos e software de segurança atualizados é fundamental para corrigir vulnerabilidades conhecidas e garantir que os sistemas estejam protegidos contra as últimas ameaças;
- Oferecer treinamentos regulares sobre segurança da informação à equipe da empresa. Isso ajuda a cons-

“Empresas que buscam se destacar precisam se adaptar rapidamente às novas e mais variadas táticas de fraude, como a criação de páginas falsas na web que se assemelham muito aos sites legítimos.

cientizar os funcionários sobre os riscos de segurança cibernética e a promover boas práticas de segurança, como evitar phishing, proteger senhas e identificar ameaças potenciais.

- Fazer backup regular dos dados críticos da empresa é essencial para garantir a recuperação rápida em caso de perda de dados devido a ataques cibernéticos ou falhas de sistema. Ainda, é importante criptografar os dados das cópias para protegê-los contra acesso não autorizado;

Por fim, um dos tópicos mais importantes para a segurança de um negócio online: desenvolver e implementar uma política de resposta a incidentes que estabeleça procedimentos claros para lidar com ciberataques, incluindo notificação a autoridades, investigação e mitigação de danos.

Investir em tecnologias de segurança avançadas, parcerias estratégicas e educação do consumidor é essencial para proteger os dados e a reputação das empresas. Somente adotando uma abordagem proativa para a segurança cibernética, as empresas podem garantir transações seguras e confiáveis durante esta e todas as outras datas.

(*) - Desenvolvimento de Negócios Sênior da Nethone (<https://nethone.com>).



kanchanachitkhamma_CANVA