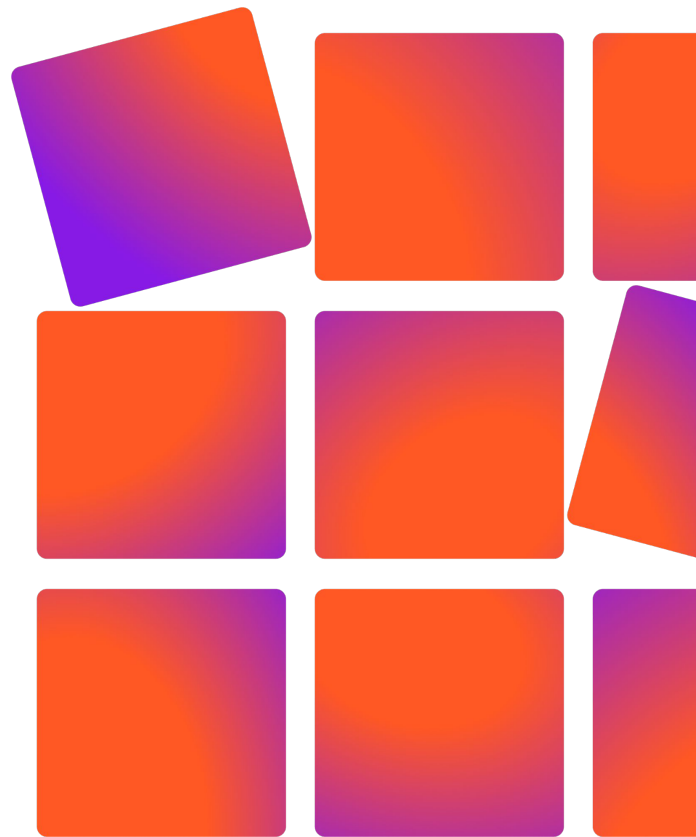


Guia Colaborativo da CTI Community:

Dicas de Segurança Cibernética para a Black Friday 2023

**Juntos, para uma
Black Friday mais
segura :)**



- 01 **Sobre este Guia**
- 02 **Dicas para Empresas**
- 03 **Dicas para compartilhar com os times internos e a família**
- 04 **Agradecimentos**

01

Sobre este guia



Guia Colaborativo da CTI Community:

Conhecimento só tem valor quando aplicado e compartilhado. E esse é o objetivo desse Guia Colaborativo construídos pelos membros da CTI Community, by Axur. O material a seguir pode contribuir com a segurança da sua empresa na Black Friday e traz também dicas para os times internos e também para todos que consomem numa das datas mais importantes do varejo mundial.

Dica: **usem sem moderação!**

A Cyber Threat Intel Community, primeira comunidade latino-americana no WhatsApp, reúne mais de 1000 profissionais de CTI. Além de contar com conteúdos exclusivos, a CTI Community é um espaço seguro para troca de informações. Todos os participantes são auditados e norteados por um Código de Conduta.

02

Dicas para Empresas





Obtenha Feedback dos Clientes

Incentive os clientes a relatar atividades suspeitas e esteja pronto para responder a esses relatórios prontamente. Esse processo pode trazer agilidade na detecção de atividades suspeitas.



Bloqueei o download de imagens

Não baixe imagens automaticamente nos e-mails. Alguns elementos gráficos podem trazer consigo códigos maliciosos ou ainda permitirem a coleta de informações como endereço IP, geolocation, camera, etc



Verifique E-mail ou Número de Telefone

Solicite que os usuários confirmem seu endereço de e-mail ou número de telefone por meio de um código de verificação enviado a eles.



Tenha regras para acesso

Implemente regras proibitivas de acesso à plataforma, mobile e API oriundos de endereços IPs de rede TOR e provedores de VPN Públicas como NordVPN, ExpressVPN, Hlde.me, VPN Unlimited, dentre outras



Faça treinamentos internos incansavelmente

Invista em educar os times internos sobre práticas seguras online, reconhecimento de phishing e procedimentos de segurança da empresa.



Use regras de Risco por localização

Implemente regras de risco para acessos oriundos de países dos quais não são o seu maior público alvo e nem há entrega/envio de mercadoria.



Ative a verificação em duas etapas nas plataformas de sua empresa

Ativar a verificação em duas etapas de todas as plataformas utilizadas na empresa é uma maneira eficaz de aumentar a segurança e reduzir significativamente as chances de um criminoso conseguir acesso.



Limite de Transações de Alto Valor

Estabeleça limites para transações de alto valor e solicite verificação adicional para tudo exceder esses limites.



Verifique a identidade dos usuários em seu e-commerce é crucial para garantir a segurança e a integridade das transações

Autenticação em dois fatores (2FA) para os clientes também ou até mesmo o uso de score de riscos que levem em conta as credenciais vazadas recentemente.



Cuide da Transparência e Comunicação

Informe aos usuários sobre as medidas de verificação que você utiliza para proteger a segurança deles. A transparência pode construir confiança e apoiar com prazos de aprovação, por exemplo!.



Revise acessos privilegiados

Quem são as pessoas da sua empresa que realmente precisam ter acessos privilegiados? Mantenha um nível mínimo de acesso aos ambientes sensíveis e com regras bem estabelecidas sobre senhas e autenticação..



Monitore Atualizações de Perfil

Esteja atento a mudanças nas informações do perfil dos usuários, como endereço de entrega, e solicite verificação se necessário



Acompanhe as Menções à sua marca em grupos utilizados por atores maliciosos

Acompanhe de forma ativa menções à marca e outros termos como esquema de aprovações, bug, virando, aprovando, testador, burlador, checker, bins em suas plataformas de Threat Intelligence. Eles indicam tendências e comportamentos atuais.



Monitore APIs

Monitore o consumo de acesso às APIs com alertas de anomalias em tempo real.



Monitore e Automatize tudo que for possível na sua operação

Se a demanda nos dias comuns já é alta, durante as datas comemorativas pode representar um desafio ainda maior. Monitore e automatizar ao máximo a detecção e remoção de perfis, aplicativos e anúncios falsos, sites de phishing....



Implemente Logs

Implemente logs que permitam uma trilha de auditoria completa, tanto para resolução de problemas, como para investigação de fraudes. Não esqueça: Endereço IP, porta lógica, timestamp, Device ID, User Agent e credencial utilizada!



Atue com playbooks pré-definidos e de forma ágil também com as credenciais

Além de ter planos para o transacional, tenha também uma tomada de ação rápida e pré-definida no tratamento de credenciais corporativas e de consumidores expostas na internet. Elas são, sem dúvida, uma das maiores fontes de fraudes e ataques hoje (que durante a Black Friday têm seu potencial de impacto aumentado)



Crie regras Anti-bots

Implemente regras antibot de monitoria e de ação em suas proteções de borda.



Revisite suas Regras de Firewall

Revise suas regras de firewall, XDR, Web Application Firewall (WAF) afim de identificar regras muito permissivas, em casos de XDR verifique as regras de exceção de modo a validar se não existe algum artefato malicioso inserido indevidamente



Monitore a Superfície Estendida

Monitore sua superfície estendida de ataque como ativos expostos sem necessidade, portas abertas indevidamente etc.



Tenha planos de Contingência

Revise e teste seus planos de contingência e recuperação de desastres. Mantenha atualizado levando em consideração as mudanças de infraestrutura recentes, assim como as de plataforma etc!



Atenção com a atualização de Servidores

Mantenha os servidores e aplicações com as atualizações de segurança em dia. Este é o momento que muitos Threat Actors se aproveitam de falhas já conhecidas para explorá-las.



Não esqueça da Validação de Backup

Valide se seu backup está funcionando corretamente, realizando testes de restore. Ele pode se fundamental em casa de ataques de ransomware, por exemplo!



Cuidado com o sequestro de estoque

Revisite suas regras de pagamento via boleto para evitar que, por uma ação mal intencionada, seu estoque fique preso e traga impacto nas vendas reais. Analise separadamente compras com valor e volume de itens altos, podem representar risco de sequestro de estoque!



Acompanhe o “aquecimento dos cartões”

Fique atento também às compras pequenas no cartão de crédito, geralmente os atores usam pequenas compras como teste e para aquecer o cartão para fraudes maiores.



Tenha Alertas acionáveis

Quanto antes você souber e agir, melhor, então monitore e crie alertas: mesmo telefone ou e-mail sendo inserido em múltiplas compras; Mesmo endereço IP ou device ID sendo utilizado para acessar diversas contas ou realizar diversas compras; Múltiplas tentativas de login com erro; Volume de transações por BIN, região, produto; Múltiplas compras de consumidores distintos para entrega no mesmo endereço/retirar em loja;



Construa e mantenha um network com outras empresas do mesmo segmento

Compartilhe eventos suspeitos e informações (como IOCs) que podem ajudar outras empresas. Além disso, consuma as informações que são compartilhadas.

03

Dicas para compartilhar com os times internos e a família





Use seu Cartão Virtual

Priorize pagamentos com cartão virtual temporário, para maior proteção dos dados pessoais. O cartão virtual gerado, pode ser descartado facilmente caso algum problema ocorra e tem menos utilidade para os atores maliciosos!



Faça sempre uma pesquisa prévia

O preço costuma chamar atenção, mas não deixe de pesquisar sobre o nome da empresa e reputação da mesma. Sites como o Reclame Aqui nos ajudam a pesquisar sobre a reputação da empresa facilmente.



Evite acessar links recebidos por email/whats ou SMS

Nunca clique em links recebidos por SMS ou de desconhecidos com ofertas "imperdíveis". Valide sempre nos sites oficiais se existe a promoção e feche direto por lá sua compra!



Valide os sites

Sites como o siteconfiavel.com.br podem ajudar você a fugir de uma verdadeira cilada digital.



Atenção ao Pagamento de Boletos

Atenção ao pagamento de boletos, verificar quem vai receber e se o nome é o mesmo do boleto e da empresa que efetuou a compra (cuidado com a troca de letras que podem passar sem você perceber).



Cuidado com as extensões instaladas nos Navegadores

A fraude do Plx, por exemplo, acontece através dessas instalações. Por via das dúvidas, não baixe nada que possa interferir na navegação. Só instale a partir dos repositórios oficiais.



Evite salvar dados do cartão

Não deixe os dados do seu cartão de crédito salvos em sites de compras. Caso alguém consiga acessar sua conta, terá facilidade de usar o cartão também!



Não abra links ou baixe anexos dos emails

Atenção ao abrir links e anexos em e-mails. Em caso de dúvidas copie o endereço do link ou salve o anexo e envie ao site <https://virustotal.com> que pode realizar uma análise técnica no conteúdo a fim de identificar se contém algum artefato malicioso.



Fique atento ao Golpe da Maquininha

Cuidado com o golpe da maquininha ao receber entregas [\(<https://idec.org.br/dicas-e-direitos/golpe-da-maquinhinha-de-cartao-6-dicas-sobre-como-se-livrar-de-um-golpe-que-se>\)](https://idec.org.br/dicas-e-direitos/golpe-da-maquinhinha-de-cartao-6-dicas-sobre-como-se-livrar-de-um-golpe-que-se)



Redobre a atenção com o Pix

Ao realizar pagamentos via PIX verifique se o beneficiário da transação é de fato o site da instituição que você realizou o pedido. Qualquer dado diferente, não finalize a transação!



Baixe somente aplicativos Oficiais

Baixe aplicativos somente das lojas oficiais. É muito comum nesta época surgir aplicativo de Black Friday, ou aplicativo de descontos de determinadas lojas, fique atento e verifique se o desenvolvedor é o mesmo do aplicativo oficial da instituição.



Tenha cuidado com compras no WhatsApp ou DMs das redes sociais

Cuidado com compras via WhatsApp ou Direct de plataformas como Facebook, Instagram e outras redes sociais.



Valide os anúncios das redes sociais

Ao clicar em anúncios publicados em mídias sociais ou em sites de busca, valide se realmente está no site da instituição, abra uma nova aba em seu navegador, acesse o site da empresa e valide se a oferta realmente é válida.



Valide o perfil/conta do SAC

Cuidado com “Perfis oficiais” de centrais de atendimento também em redes sociais e whatsapp. Valide se o endereço do perfil ou o telefone são os oficiais das instituições, estas informações estão disponíveis nos sites de cada empresa.



Cuidado com ligações de Centrais

Cuidado com ligações de supostas centrais de atendimento de instituições financeiras com o discurso de validar uma transação PIX agendada, pagamentos, transferências, dentre outras. Na dúvida, desligue e ligue para o número de sua instituição que pode ser obtido nos aplicativos e sites oficiais.



Habilite sempre o 2FA

Habilite o segundo fator de autenticação em todas as redes sociais, plataformas e e-mail que tiver e evite, sempre que possível, o SMS como segundo fator de autenticação. Se puder, use o email de alguém de confiança.



Não faça pagamentos de testes ou de cupons

Nenhuma empresa irá solicitar para o cliente realizar uma transação PIX, transferência ou pagamento para testes ou para envio de cupons, bem como não irá solicitar para o cliente instalar um programa antivírus ou similar.



Não caia no golpe do Presente

Cuidado com o golpe do presente (<https://blog.nubank.com.br/golpe-do-presente-falso/>)

04

Agradecimentos



OBRIGADO!

Um super agradecimento a todos que contribuíram para a construção deste guia colaborativo, com dicas e também com a sua revisão.

Compartilhar conhecimento fortalece nossa comunidade. Juntos, estamos construindo algo incrível :)

Obrigado pela sua participação! 🌐🚀

**Um obrigado mais que especial aos
top 7 participantes:**

- Jefferson Lima
- Rogério Nicolete
- Rachel Bullmann
- Alison Juliano Pagnoncelli
 - Antônio Cruz
 - Diego Silva
- Silvana Tavares

Vamos fazer parte e criar, juntos, a melhor comunidade de CTI do Brasil e do mundo? :)

axur.to/community

