

Como não ser mais uma vítima do Black Friday no E-commerce de 2019?

O Black Friday, febre no Brasil, atrai milhares de pessoas para os sites de e-commerce, em busca de grandes descontos. É nesta época, porém, que muitos golpistas e fraudadores digitais lucram muito com a ganância e inocência de algumas pessoas. Saiba como não se tornar mais uma das milhares de vítimas do Black Friday, adotando 7 (sete) medidas simples.

Anualmente os brasileiros contam os dias e as horas para que as lojas anunciem o Black Friday, que faz sucesso por aqui desde 2010, ocorrendo na quarta sexta-feira do mês de novembro, inspirado pela tradição Norte Americana.

Como vínhamos falando há algum tempo, o crime digital brasileiro é muito mais criativo do que técnico, e tem hoje recursos de hospedagem anônima e registro de domínios protegidos por proxies, além de outras técnicas e recursos simplificados que lhes permitem subir um site com uma facilidade extrema. Assim, nesta época, todo o cuidado é pouco com as lojas virtuais “fakes”, falsas ou “anônimas” e é nesta última aonde existe muita dificuldade em identificar seus criadores.

Observamos que os criminosos digitais inovam constantemente e hoje dominam técnicas de SEO (*Search Engine Optimization*), analisam sites parecidos com os que vão subir em analisadores de tráfego e logo posicionam seus sites nos buscadores como

uma das primeiras opções locais, regionais ou nacionais.

Sem contar que as redes sociais e buscadores não fazem distinção de criminosos que impulsionam seus sites em períodos de fortes vendas no e-commerce, o que faz com que as vítimas continuem expostas cada vez mais a sites falsos, cujo escopo é roubar o dinheiro do comprador.

Para evitar ser vítima de golpes na época do Black Friday, apontamos 7 (sete) pontos focais que se adotados, minimizam as chances de um dissabor na hora da compra de produtos com descontos:

1. **Pesquise antes:** Faça uma análise minuciosa da loja, site, endereço físico, sócios, reclamações, telefones, se possível faça um contato telefônico, busque referências; Acesse o histórico de reclamações no procon ou mesmo no consumidor.gov.br; Utilize um site de WHOIS (Como <http://whois.domaintools.com/>) para verificar dados do registro do domínio;
2. **Fuja de transferência bancária:** Bandidos querem seu dinheiro rápido e não querem trabalho. Não vão oferecer opções que você possa cancelar no futuro. Portanto, desconfie de sites que só aceitam boletos ou transferências bancárias, prefira sempre meios seguros de pagamento onde o dinheiro só é liberado após a entrega da mercadoria;
3. **Visite o site de interesse agora:** Isso mesmo, antes do Black Friday. Veja se ele já está no ar, os produtos, os preços, faça prints de tudo, de preferência utilize até mesmo o Original.My para registrar algo de interesse. No BlackFriday, compare para verificar se houve um “aumento para baixar posteriormente”;
4. **Não compre por links:** Recebeu um link por e-mail, Messenger, WhatsApp e está pensando em clicar nele e

comprar? Não seja tolo! Você vai ser enganado, perderá seu dinheiro e seus dados. Acesse sempre diretamente o site da loja e verifique se a mesma é segura e se o certificado digital está expedido para ela mesma e não para outra empresa.

5. **Proteção de dados e políticas:** Avalie se o site está em conformidade com a Lei de Proteção de Dados, se cumpre as entregas, garantias, se está auditado e reconhecido com selos e certificados (Como o Legal2you da CyberExperts, que comprova o compliance do site) e desconfie de dados em excesso solicitados para uma simples compra.
6. **Cuidado com selos falsos:** Os bandidos vão tentar passar credibilidade do site para roubar seu dinheiro e para isso, vão usar falsos selos de sites seguros ou que estão em conformidade com a Lei. Desconfie, vá até o site do selo e confirme se a loja realmente é certificada ou não.
7. **Registre as provas:** Desde o momento de iniciar a transação, fornecendo dados até a conclusão da compra, registre tudo, telas, confirmações, e-mails recebidos. Hoje existem vários programas “screen recorders”, alguns até nativos do sistema operacional, que registram com metadados atividades no computador. Todos estes dados serão úteis para comprovação da compra e até mesmo para se apurar a autoria.

Deste modo, é preciso ter em mente que descontos “*fora da realidade*” podem ocultar um site falso, fraudado, upado apenas para lesar e em seguida ser removido do servidor web, sem qualquer rastro da fraude. Bandidos normalmente usam registros de domínios em nome de pessoas laranjas, não possuem empresa constituída e usam telefones celulares “chips frios” e números VOIP para contato, que após

o golpe são abandonados.

O consumidor precisa ter em mente que o Marco Civil da Internet, Lei 12.965/2014, permite e dá a base para que seja possível apurar os responsáveis por um golpe ou fraude digital envolvendo sites “falsos” ou aparentemente anônimos, sendo que os provedores de hospedagem deverão guardar os registros de acesso à aplicação por 6 (seis) meses. Para hospedagem internacional (muito utilizada por bandidos), o consumidor deve buscar um escritório especializado em direito digital ou advocacia envolvendo crimes cibernéticos, para que possa adotar as medidas para apuração da autoria.

Não bastasse, o site pode ser “oficial” e até honesto, mas maquiado o preço, o que pela lei brasileira é considerado propaganda enganosa, razão pela qual a orientação é que pesquise sempre os preços com antecedência. Sites como Zoom, BlackFriday, Buscapé, Já Cotei, dentre outros disponíveis que costumam trazer comparativos e evolução de preços. Se encontrar o “subiu para dar desconto”, muito comum também na oferta de serviços, cursos e treinamentos, acione o Procon, Reclame Aqui e demais órgãos de proteção ao consumidor da sua região.

Para as lojas, é preciso ficar atento pois o Procon vem apurando lojas que fazem “sobe e desce” de preços, bem como é preciso um cuidado especial em relação a “fakes” que surgem na época do

BlackFriday e usam a marca da loja indevidamente, lesando consumidores, monitorando as redes sociais e principalmente, sendo transparentes para com os clientes, alertando os riscos da época e detalhes das ofertas, nos moldes do artigo 31 do Código de Defesa do Consumidor.

O IDCI, Instituto de Defesa do Cidadão na Internet, é um instituto que atua por meio da sua equipe em todo o país, analisando sites ligados a fraudes e divulgando aos cidadãos, inclusive, recebendo denúncias de sites “falsos” ou que estão descumprindo a Lei, sobretudo neste período crítico e que envolve muitas transações digitais, que é o Black Friday. Do mesmo modo, em São Paulo, o PROCON organiza uma lista de sites não confiáveis, atualizada diariamente. Acesse <https://sistemas.procon.sp.gov.br/evitesite/list/evitesites.php> e confira se o site se encontra nesta lista. Se estiver lá, fuja!

Fique atento, siga IDCI e receba informações em tempo real sobre golpes e fraudes no comércio eletrônico e formas de proteção. O cidadão pode consultar o IDCI para dúvidas e reclamações pelos seguintes canais de atendimento: pelo WhatsApp (11) 98459-7777 (de segunda a sexta das 8h às 20h e aos sábados das 8h às 14h; Ou ainda pelo Facebook (www.facebook.com/pages/IDCIBrasil)).

No meu canal no youtube (youtube.com/josemilagre) semanalmente, eu trago muito conteúdo sobre direito e segurança digital. Se inscreva para receber avisos sobre os vídeos gratuitos, que são publicados semanalmente.