Black Friday 2020: Especialista em crimes digitais, José Antonio Milagre, orienta como evitar golpes virtuais e como agir caso tenha sido vítima.

Mais uma BlackFriday se aproxima e com ela o oportunismo de criminosos cibernéticos, que usam de técnicas variadas para aplicação de golpes, explorando muitas vulnerabilidades dos consumidores virtuais, que desatentos, acabam fornecendo dados pessoais ou comprando em páginas falsas, que são criadas apenas pelo período necessário para tirar o dinheiro do consumidor. Esta edição, porém, promete ser maior por conta do isolamento social diante da COVID-19. Segundo a Ebit Nielsen, as vendas devem crescer 27% em comparação com a edição de 2019.

Os criminosos digitais têm criado "lojas iscas", normalmente hospedadas em servidores no exterior. Do mesmo modo, ocultam os dados do registrante, por meio de registros *"domain by proxy"*, tudo para dificultar a investigação de quem está por trás do e-commerce "simulado".

Rapidamente investem em anúncios nos buscadores e outros métodos de impulsionamento, incluindo redes sociais e rapidamente ficam bem ranqueados na rede. A vítima então se depara com o anúncio, normalmente com preço fora do comum. Se não se atentar para elementos visuais da página ou dados de contato da loja, acaba acreditando que está fazendo um bom negócio, e nunca mais verá seu dinheiro.

As lojas falsas, normalmente se valem de depósito bancário ou

boletos, que dificultam o cancelamento das compras ou o rastreio do dinheiro. Assim, todo o cuidado é pouco no período de promoções, já que o crime digital brasileiro explora momentos de grande mobilização digital para auferir lucro, lesando pessoas.

O advogado e perito especialista em crimes cibernéticos, José Antonio Milagre, CEO da CyberExperts e Diretor do Instituto de Defesa do Cidadão na Internet (IDCI) apresenta estratégias para se proteger de golpes digitais e dá dicas sobre como agir, caso tenha sido vítima de fraudes e crimes cibernéticos na BlackFriday.

Dez estratégias para que não que seja vítima de golpes digitais na BlackFriday:

1) Cuidado com descontos absurdos. Embora seja Blackfriday, 90% de desconto é algo estranho de se ver. Cuidado, confira a média de preço dos produtos. O criminoso vai usar este gatilho para chamar sua atenção;

2) Avalie a reputação da Loja. Em um universo de aproximadamente 1 milhão de lojas virtuais, muitas delas podem ser "lojas iscas", criadas para ficar no ar por pouco tempo, fazer centenas de vítimas e desaparecer. Portanto, pesquise se a loja tem "histórico", comentários, outras compras, etc. O Google está aí para isso;

3) Avalie as formas de pagamento. Desconfie de lojas que só oferecem depósito bancário, boleto ou criptomoedas. Estas modalidades podem dificultar o cancelamento da compra ou a investigação dos destinatários. Opte sempre por meios de pagamento seguros, onde o dinheiro é liberado quando o consumidor declara que recebeu a mercadoria;

4) Busque contatos da loja. Faça contatos prévios com a loja, mas não só por e-mail, busque um contato telefônico, verifique onde está a sede e desconfie de lojas onde o único contato é um telefone celular;

5) Cuidado com ofertas em comunicadores, e-mails e redes sociais. Jamais clique ou acesse lojas virtuais a partir de links, ou ofertas que receber em comunicadores, WhatsApp e redes sociais;

6) Não acesse lojas pelo buscador. Acesse diretamente o site da loja evitando também pesquisar pela loja no buscador. Cuidado com pequenas mudanças no nome do site e avalie se possui certificado digital expedido para o próprio site. Os criminosos digitais podem falsear um link direcionando a vítima para o site errado. Ataque de pishing são muito comuns, com a falsificação de marcas e identidade visual de sites com ofertas de descontos, dentre outras chamadas para pescar consumidores desatentos;

7) Cuidado com códigos enviados para o celular para supostos descontos. Imagine que você recebe uma mensagem que conseguiu um cupom especial para o BlackFriday, mas para que você receba, você precisará informar um código que chegará pelo celular via SMS. Neste exato momento a vítima não ganhou o desconto, mas pode ter permitido a clonagem do WhatsApp ou até mesmo ter o reset de senhas de app's financeiros realizados com sucesso, dando acesso ao criminoso. Não confie jamais nesta abordagem. Não informe a ninguém códigos que receber pelo celular;

8) Golpes com PIX. Muitos criminosos também poderão explorar este momento envolvendo a novidade, falsear identidade visual de lojas e oferecer produtos com "desconto" para compras com o pix, oferecendo códigos errados ou chaves que direcionarão o pagamento para o fraudador. Muita cautela no uso da nova tecnologia;

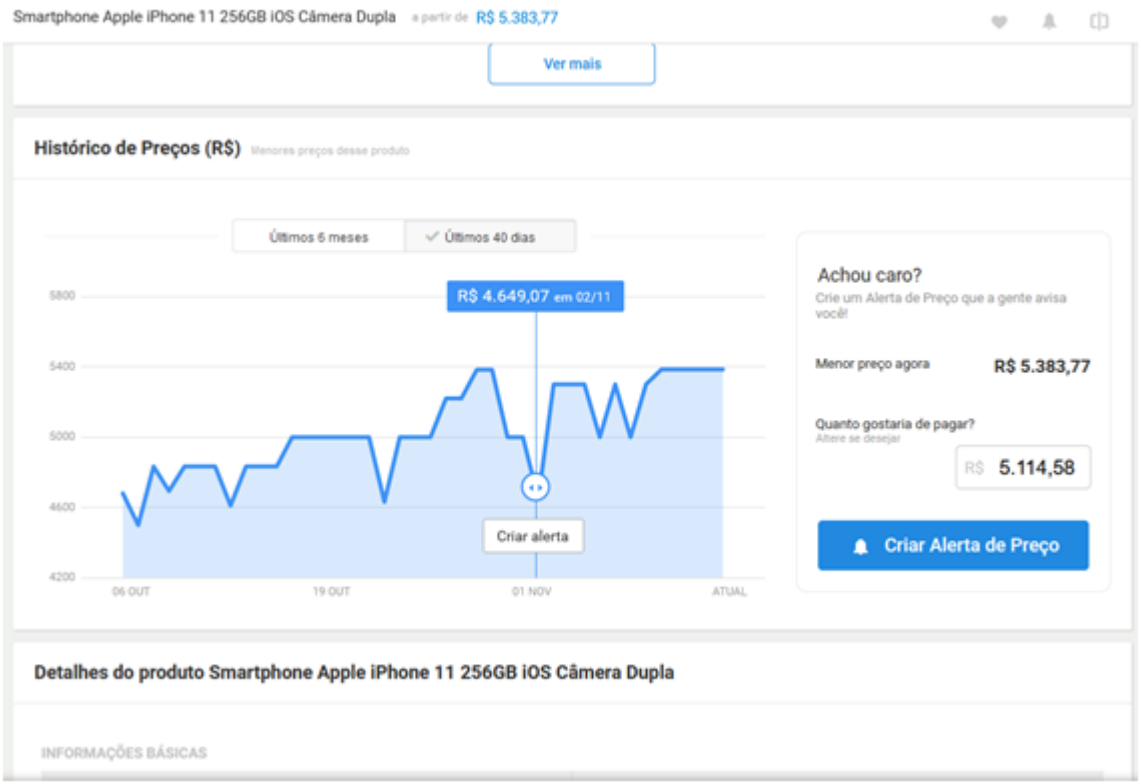
9) Desconfie de dados excessivos. Cheque a política de privacidade do site, se conecte a partir de uma conexão segura, avaliando se o site também tem SSL (https) assegurando proteção contra interceptação de dados e jamais forneça dados mais que necessários para a compra, como "senha do cartão" e

outros dados. Mantenha sempre seu sistema operacional atualizado, com firewall e anti-malware ativados;

10) Faça provas de tudo. Guarde provas de toda a compra, salve os códigos, registre prints, e-mails recebidos, se necessário registre em vídeo do processo de compra. Todos estes dados podem ser uteis diante de uma fraude ou golpe, onde a perícia digital poderá identificar a autoria dos criminosos.

Avaliar aspectos de legalidade de um site nem sempre é uma tarefa fácil para o consumidor. Embora a Lei Geral de Proteção de Dados já esteja em vigor (LGPD), já esteja em vigor, muitas lojas ainda não estão em conformidade e não são totalmente transparentes em seus processos.

Outra proteção importante, mas não realizada a golpes digitais, é avaliar as chamadas “fraudes” de lojas que sobem o preço para depois baixarem. Para isso sites como buscapé, zoom e baixou agora podem auxiliar, pois, apresentam um histórico do preço.



Buscapé mostra preço do Iphone 11 em 02/11 e 14/11 de R$ 4649,07 por R$ 5383,00

Caso tenha sido vítima de um golpe digital, o especialista, José Antonio Milagre, recomenda: "Imediatamente *resgate todos os dados da compra, registre um boletim de ocorrência online e procure um especialista em direito digital e crimes cibernéticos para que se incie um processo de apuração da autoria e responsabilização dos criminosos. Em casos de clonagem do chip, pode-se buscar a reparação em face da operadora de telefonia móvel.*"

Do mesmo modo é muito importante contactar o banco com informações sobre a fraude e notificar a loja que eventualmente teve a marca usada para a fraude, para se buscar uma resolução amigável. As lojas podem ser responsáveis, se não adotavam medidas de segurança da informação ou não monitoravam o uso indevido de suas marcas, permitindo que fossem usadas para fraudes e golpes.

Porém, é importante advertir, se a loja comprovar que não deu causa ou que a despeito de todas as ostensivas demonstrações de segurança, a culpa foi exclusiva do consumidor, esta pode não se obrigada a reparar. Cada caso é um caso, e muitos deles serão apreciados pela Justiça. Por isso, prevenção é a melhor opção, sempre.

O IDCI (Instituto de Defesa do Cidadão e Consumidor na Internet) presta atendimento e apoio a vítimas de golpes e crimes cibernéticos, por seus canais, Siga @idcibrasil no Facebook e Instagram.

Prof. MSc. **José Antonio Milagre**, é Advogado e perito especializado em Direito Digital e Crimes Cibernéticos, Mestre e Doutorando Ciência da Informação pela UNESP, Presidente da Comissão de Direito Digital da OAB/SP Regional da Vila Prudente, Autor pela Editora Saraiva em co-autoria com o Professor Damásio de Jesus, dos livros "Marco Civil da Internet: Comentários à Lei 12.965/2014" e "Manual de Crimes Informáticos". Fundador do Instituto de Defesa do Cidadão na Internet – IDCI.

Canais:

http://www.instragram.com/drjosemilagre
http://www.facebook.com/drjosemilagre
http://www.youtube.com/josemilagre