BLACK FRIDAY: Quais os cuidados que devemos tomar para não cairmos em golpes?

A famosa "BLACK FRIDAY" que ocorre nos Estados Unidos, antecedendo as compras de finais de ano com descontos atrativos, também se tornou comum no calendário brasileiro e em outros países.

Como não poderia deixar de acontecer, muitos países acabaram se espelhando nesta data comemorativa do varejo americano e também fazem suas liquidações. No Brasil, também vemos inúmeras lojas (online e físicas) já divulgando suas promoções de *Black Friday*, a fim de atraírem os consumidores para as compras natalinas.

Enquanto muitas empresas estão se preparando para lançar as promoções na *Black Friday*, muitos cibercriminosos também preparam seus golpes.

São inúmeros *phishing scam* espalhados pela internet e redes sociais, a todo o momento, que se aproveitam de datas comemorativas do comércio para fisgarem os mais desatentos.

Você sabe o que é *phishing scam*?

É um e-mail, mensagem (via SMS, Whatsapp, mensagem direta nas redes sociais, etc) ou página (fanpage no Facebook, perfil em rede social, site, blog, etc) falso, que tem o intuito de se passar por terceiro (uma conhecida rede de varejo, por exemplo), divulgando informações inverídicas, mas extremamente atrativas para quem as recebe, que estimula o usuário a clicar neste conteúdo. Uma vez que o indivíduo clica no material recebido, geralmente é instalado um código malicioso em seu dispositivo (celular ou computador), que acaba capturando os dados digitados e trafegados naquele aparelho. Assim, o fraudador poderá ficar sabendo, por exemplo, das senhas digitadas em redes sociais, contas bancárias, e-mails, conteúdo enviado/recebido e outros dados pessoais armazenados no dispositivo. Geralmente o usuário não percebe qualquer alteração em seu dispositivo: ele clica em um link recebido ou na página em questão e nada acontece, mas a fraude já está ocorrendo em 2º plano.

É desta forma que ocorrem grande parte das invasões a dispositivos informáticos e vazamentos de dados pessoais.

Como que o fraudador consegue obter esse clique do usuário? Simples. Basta atrair a atenção do seu alvo: utilizar o assunto do momento – "Black Friday", por exemplo – ou qualquer outro fato curioso, polêmico, e vinculá-lo a um conteúdo visualmente atrativo, que pareça verídico. Exemplo típico de fraude na *Black Friday*: uma promoção de um produto por um valor extremamente inferior ao preço real, hospedada em uma fanpage falsa de uma grande loja de eletrônicos, com identidade visual semelhante. O consumidor, atraído pela oferta sedutora, clica no link rapidamente, efetua a compra, paga o boleto

bancário e tempos depois, quando não recebe o produto, percebe que caiu em uma fraude. Só neste momento é que ele vai perceber que o endereço da página onde comprou era diferente da página oficial daquela rede de lojas, que o valor do produto no site oficial desta rede era diverso, que o boleto emitido estava em nome de terceiro desconhecido sem qualquer relação com este varejista... Aí já é tarde, ele já caiu no golpe. Resta registrar um Boletim de Ocorrência e aguardar o desfecho do caso.

Esse tipo de situação ocorre com frequência e tal fato pode ser considerado um crime de **estelionato**, previsto no art. 171 do Código Penal:

> *Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:*
> *Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.*

No exemplo citado acima, a fraude eletrônica estará configurada a partir do momento em que a vítima efetuar o pagamento da transação bancária. Portanto, será vítima da fraude somente o indivíduo que de fato teve prejuízo financeiro. O simples recebimento de mensagens de cunho fraudulento, sem que o destinatário sofra efetivamente qualquer prejuízo, não caracteriza o crime de estelionato, pois esta conduta estará no âmbito da tentativa.

Os criminosos estão se sofisticando cada vez mais, criando sites e páginas em redes sociais cada vez mais parecidos com lojas virtuais renomadas, hospedados em domínios fraudulentos, no intuito de confundir o consumidor, atraindo assim mais pessoas, a fim de aplicar mais golpes ou obter mais dados pessoais.

Se você pesquisar por “Black Friday” e outros termos relacionados nos principais buscadores da internet, com um pouco de atenção, certamente já irá se deparar com essas páginas falsas.

Portanto, todo o cuidado é pouco! Fique atento para que sua “Black Friday” não se transforme em uma grande dor de cabeça.

Para evitar cair em fraudes eletrônicas, atente-se à estas dicas:

1. Instale um ótimo antivírus em seu computador e em seu celular (sim, é muito importante que seu celular também possua antivírus de varredura instantânea. Há bons antivírus gratuitos nas lojas de aplicativos, e há excelentes antivírus pagos por valores menores do que você imagina). Habilite a

pesquisa segura para este antivírus: o software poderá alertar-lhe sobre eventuais sites nocivos/invasivos quando você estiver navegando na internet.

2. Não abra todo conteúdo que recebe, principalmente se tiver um link, mesmo que seja mensagem enviada no grupo da família via Whatsapp. (Pode ser um *phishing scam* (ou uma *fake news)* encaminhado por alguém que não tem ideia desse risco).

3. Desconfie de todos os e-mails recebidos. Verifique se o endereço do remetente do e-mail é conhecido, se tem relação com o conteúdo enviado, se o domínio do e-mail tem relação com o site vinculado àquela oferta.

4. Pare o mouse sobre o link e não clique, apenas observe o link que se forma: **geralmente os links fraudulentos são extensos e/ou possuem uma terminação sem qualquer relação com a loja virtual pela qual tentam se passar**. Portanto, se o conteúdo do e-mail fizer menção a uma determinada loja, mas o link que aparece não está relacionado a mesma loja/marca, pare por aí!

5. Veja se a página da loja virtual onde você vai comprar é segura, se possui certificado digital com a menção "https".

6. Observe se há erros de ortografia/gramática. Páginas, e-mails e mensagens fraudulentas geralmente deixam passar batido os erros de português.

7. Utilize um navegador que em suas políticas de privacidade bloqueie o rastreamento de seus dados pessoais por sites considerados invasivos.

8. Desconfie de anúncios com preços muito inferiores aos praticados pelo mercado. Não acredite em promoções fenomenais.

9. **Procure pela página ou site oficiais da marca/loja. Confira se aquele anúncio é real** (grandes marcas possuem um selo de verificação em suas páginas nas redes sociais). Compare os preços no site da marca/loja e no link divulgado em questão. Não compre diretamente dos links divulgados em páginas/perfis de redes sociais ou enviados através de mensagens: a maioria dos fraudadores cria perfis fraudulentos nas redes sociais, copiando grandes marcas, na tentativa de ludibriar o público. Veja se o endereço da página divulgado no anúncio confere com o endereço da página oficial. Observe o link que aparece em seu navegador.

10. Verifique se o site consta na lista negativa do PROCON de seu Estado.

11. Pesquise pelo nome da loja nos buscadores da internet e sites como o "Reclame Aqui". Veja se há comentários negativos nas redes sociais vinculadas à loja em questão.

12. Ao receber um e-mail de ofertas, tome as mesmas precauções e não clique em qualquer link, pois poderá ser instalado um código malicioso em sua máquina, que poderá danificar seu dispositivo, monitorar sua navegação ou capturar seus dados.

13. Todo o cuidado é pouco! Confira sempre ANTES de comprar! Verifique sempre no site da loja/marca se aquela campanha publicitária/promoção é real, quais são as condições de pagamento e de envio do produto. Se faltarem informações, certamente é porque aquela oferta é falsa.

14. Havendo qualquer dúvida ou notando alguma divergência, não prossiga com a compra. Encaminhe o anúncio recebido para o site oficial da marca/loja, denuncie a fanpage/perfil para a rede social.

Caso você perceba que caiu em uma fraude eletrônica, tome as seguintes providências:

1. Armazene o anúncio que foi objeto do golpe: salve o e-mail original recebido, mantenha as mensagens recebidas, tire prints do anúncio publicado em rede social ou site com os respectivos links.

2. Guarde o(s) comprovante(s) de pagamento(s): boleto bancário recebido e respectivo comprovante, fatura do cartão de crédito, comprovante de depósito ou transferência bancária/PIX, etc.

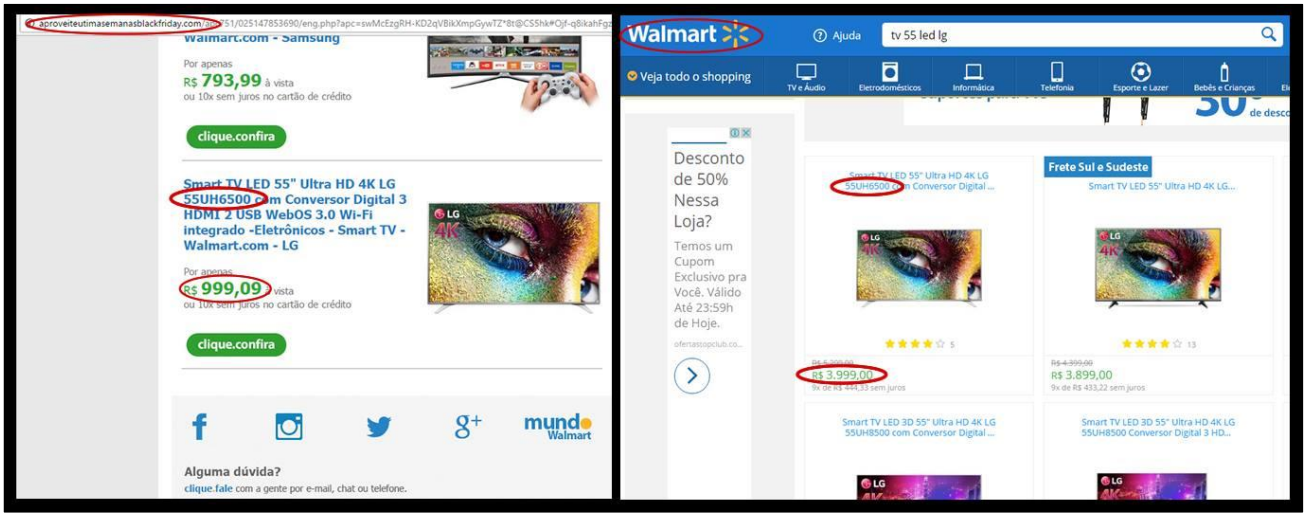
3. Armazene toda e qualquer comunicação recebida durante e após o processo de compra (e-mails, mensagens, etc.).

4. Com estas provas também salvas em mídia eletrônica própria (ex: pendrive), **registre um Boletim de Ocorrência eletrônico ou na delegacia mais próxima de seu endereço**, pela prática do crime de estelionato. Caso sua cidade possua delegacia especializada em Crimes Eletrônicos, confira se tal delegacia atende especificamente este tipo de ocorrência.

5. Após o registro do Boletim de Ocorrência, dependendo do tipo de situação, se o golpista já for identificado, **você poderá ingressar diretamente com uma ação junto ao Juizado Especial Cível (JEC) e Juizado Especial Criminal (JECrim),** na tentativa de obter-se o reembolso do prejuízo causado, e também no intuito de punir o indivíduo pela prática do delito. Estas ações judiciais propostas perante os Juizados Especiais possuem um limite específico de valor para ressarcimento, não necessitam de advogado para seu acompanhamento e não requerem pagamento de custas judiciais.

6. Com as provas em mãos, você poderá entrar em contato com um(a) advogado(a), para que ele(a) possa avaliar outras medidas cabíveis, caso você não queira agir por iniciativa própria perante o JEC ou JECrim.

**Na imagem abaixo: à esquerda, exemplo de um site falso, c/ anúncio fraudulento; e à direita, site original c/ oferta real.*



Gisele Truzzi

Advogada especialista em Direito Digital e Segurança da Informação

CEO e sócia fundadora de [Truzzi Advogados]