Como proteger as compras online durante a Black Friday?

publico.pt/2020/11/13/impar/noticia/proteger-compras-online-durante-black-friday-1939081

Carla B. Ribeiro

Vem aí mais uma *Black Friday* e, desta vez, é expectável que as compras se concentrem online – e os roubos também.

Com o confinamento e o aumento de compras online, os riscos de ser enganado são maiores. A Visionware é uma empresa portuguesa que tem o seu foco na cibersegurança. E, criada há 15 anos, teve este ano mais procura do que nos 14 anos anteriores. A explicação, segundo Bruno Castro, CEO do projecto, está relacionada com os condicionalismos impostos pela pandemia: **"Fomos todos obrigados a ir viver para o mundo digital"** e "fazemo-lo em casa, onde estamos mais vulneráveis". "Em casa, por um lado, baixamos a guarda, por outro, temos mais distracções e estamos menos focados, o que nos pode levar a clicar num *link* ou abrir um e-mail de *phishing*."

Certo é que, por estes dias, as tentativas de *phishing* aumentaram, até porque muitos negócios optaram por alargar as promoções da Black Friday de dia 27 a um período que se iniciou já no início do mês. "O que acontece é que quando se clica no *link* 'errado' abre-se uma porta para o nosso computador, num processo que vai recolher todo o tipo de informação", detalha Bruno Castro. E, ao contrário do que sucede com os "vírus de guerra", que visam revelar fragilidades de serviços ou de instituições, **"os vírus de roubo são silenciosos".**

Depois, continua o mesmo investigador,
há o engodo de promoções
fantásticas que, por estar a decorrer a *Black Friday*, muita gente não desconfia:

"Ninguém vai torcer o nariz a uma promoção *last minute*". E, por vezes, até se usa o nome de uma empresa conhecida. Nestes casos, relata o especialista, o que acaba por se dar são **dois roubos: o primeiro, com o dinheiro da venda, sendo que o produto nunca chega a quem o adquiriu, e, o segundo, com os dados do cartão de crédito** — e estas informações são usadas no mesmo período em que há uma grande confusão de compras, tornando difícil o rastreamento em tempo real.

Estes exemplos não são novidade, mas, com praticamente toda a gente concentrada no fazer a sua vida online, mesmo sem conhecimentos para tal, esta *Black Friday* promete bater recordes no número de fraudes. **"Para quem vive de roubar online é como roubar doces a crianças."**

A Associação Portuguesa de Bancos, que entretanto publicou um vídeo explicativo de como nos podemos proteger online, avança dados da SIBS sobre a Black Friday, alertando para o facto de, em 2019, ter representado "10% do total de compras online" e prevendo que se verifique, este ano, "um crescimento de 30% a 50% nas vendas durante este período".

Entre as regras básicas para evitar cair na armadilha, Bruno Castro aconselha que os utilizadores do mundo digital adoptem a mesma postura que têm no mundo real, como **não circular à noite sozinho por locais desconhecidos ou não falar com estranhos**.

Além das duas ideias apresentadas, que considera essenciais, aconselha a desconfiar de promoções fantásticas que cheguem através das redes sociais ou de canais de comunicação como o WhatsApp e **procurar informação sobre quem está a vender** antes de efectuar quaisquer compras, através de uma pesquisa em qualquer motor de busca ou procurando dados em sites específicos, que avaliam a credibilidade de determinado endereço na web: casos do Urlvoid, do Talos ou do ThreatCrowd.

Além disso, refere, **é sempre de desconfiar quando o único meio de pagamento disponível é o cartão de crédito**: "Meios como o PayPal ou o MBWay obrigam ao pagamento de comissões; quem está a roubar não vai andar a gastar dinheiro nisso", contextualiza.

Como evitar a fraude online

- Não utilizar redes públicas (ex.: *hotpots wifi*);
- Não abrir e-mails ou SMS de remetentes desconhecidos com promoções da *Black Friday*, seja no contacto pessoal, seja no corporativo;
- Não clicar em *links* ou transferir documentos suspeitos;
- Não clicar em anúncios online, optando por contactar as marcas pelos canais oficiais;
- Não fazer compras através de redes sociais, sem validar a veracidade das marcas;

- Não fazer compras em sites duvidosos, confirmando sempre o certificado SSL dos sites onde navega (identificado através do cadeado do lado esquerdo e referência HTTPS), tendo a consciência de que também estes elementos podem ser manipulados pelos criminosos;
- Ser céptico em relação a ofertas particularmente excepcionais ou que pareçam feitas à sua medida;
- Não ceder dados pessoais, nomeadamente aqueles que sejam particularmente sensíveis ou desnecessários à operação de compra a efectuar;
- Optar por formas de pagamento seguras, por exemplo através de cartão temporário gerado pela MBWay ou transferências bancárias, evitando o registar dados bancários;
- Ter atenção aos cupões que chegam por WhatsApp e redes sociais. Ser cuidadoso ao clicar em *banners* e *pop-ups*;
- Opções de pagamento: Desconfiar sempre se o site aceita apenas cartão de crédito como forma de pagamento;
- Guardar as provas que demonstram o que estava anunciado e a navegação pelo site e da própria compra;
- Fixar um limite máximo para gastar numa compra; reduza o montante disponível nos cartões para os pagamentos online;
- Limite as tentativas de transacção do seu cartão bancário;
- Reduzir a quantidade de fundos nas contas bancárias ou utilizar um cartão pré-pago de débito para os pagamentos online;
- Activar e utilizar sempre a autenticação de dois factores (Verified by Visa, MasterCard Secure Code, etc.).

Notícia actualizada com informação veiculada pela Associação Portuguesa de Bancos