Sugestões para compras seguras durante a quadra festiva para os retalhistas

As compras na época festiva estão a todo vapor e os retalhistas de todo o mundo estão a preparar-se para o aumento de encomendas que ocorre nas semanas antes. À luz dos desafios que os retalhistas enfrentam, **é essencial priorizar os riscos de cibersegurança.**

Abaixo estão as sugestões de preparação cibernética que os retalhistas devem seguir para **manterem a segurança** durante as compras online.

Sugestão 1 Mantenha o software atualizado

- Ative as **atualizações automáticas** para todo o software.
- Cada atualização contém as correções e os patches mais recentes, que podem protegê-lo contra ameaças potencialmente perigosas.
- **Reiniciar o seu computador** é também outra forma de garantir que os patches são instalados.

Sugestão 2 Defina as suas políticas de cibersegurança

- **Forme todos os seus colaboradores** nas suas políticas de cibersegurança.
- Mostre aos seus colaboradores a importância da cibersegurança e o papel que desempenha nas suas vidas pessoais e profissionais.
- **Inscreva-se no nosso Programa de preparação cibernética gratuito** e obtenha acesso a outros recursos do CRI para desenvolver bons hábitos de preparação cibernética.

Sugestão 3 Deixe de usar as pens USB

- As pens USB são úteis para partilhar ficheiros entre computadores, mas também podem ser usadas para transmitir **vírus e malware**.
- Configure um **computador de rede não empresarial** que pode ser usado para verificar se há malware nas pens USB e remover as informações das unidades.
- Adote um **sistema de partilha de ficheiros online ou baseado na nuvem** que esteja protegido por acesso, para que não necessite de utilizar uma pen USB.

Sugestão 4 Esteja atento ao phishing nas épocas festivas

- **Fique atento a esquemas de phishing** e mensagens maliciosas que tentam tirar proveito de compradores ocupados e distraídos.
- Verifique o endereço de e-mail do remetente e **reveja os e-mails com cuidado** para se certificar de que o remetente é legítimo. Se parece bom demais para ser verdade, provavelmente é!
- **Nunca clique em ligações**, transfira anexos ou responda a informações de remetentes desconhecidos! Mesmo que você "conheça" a pessoa, é sempre bom enviar uma mensagem ou telefonar-lhe para conferir antes de agir.

Sugestão 5 Mantenha as palavras-passe seguras

- Certifique-se de que as frases de acesso **são fortes e únicas** para cada conta.
- Ative a **autenticação multifator (AMF)** em todas as suas contas, se estiver disponível.
- Nunca divulgue as suas palavras-passe a ninguém e **altere sempre as suas palavras-passe após viagens** ou atividades em que inicie sessão numa conta num dispositivo de outra pessoa.