CYBER READINESS
INSTITUTE

# Saudações festivas! Sugestões para se manter ciberseguro durante a época festiva

Durante toda a época festiva, as empresas e os consumidores estão em risco no que toca aos ciberataques. Muitas organizações governamentais, incluindo o FBI, a Agência de Segurança de Infraestruturas Críticas (CISA) e o Centro Nacional de Cibersegurança do Reino Unido, divulgaram orientações sobre as melhores formas de se manter seguro durante esta quadra festiva. O Cyber Readiness Institute (CRI) reuniu os destaques desses avisos num guia para a época festiva em duas partes destinado aos consumidores e retalhistas.

## Consumidores

### Esteja ciente de que os hackers estão sempre à procura das formas mais eficientes de chegar a si.

Os esquemas de phishing (ou smishing) através das mensagens de texto (SMS) durante a época festiva quase duplicaram em relação ao ano passado, de acordo com um relatório divulgado pela Proofpoint.

Os hackers enviam mensagens de texto e e-mails **replicando notificações de entrega**, notificações de monitorização ou ofertas da época festiva.

### Melhores práticas:

- Verifique os seus dispositivos: Utilize palavras-passe fortes ou frases de acesso secretas de pelo menos 15 carateres, atualize o seu software e ative a autenticação multifator.
- Compre apenas através de fontes fidedignas: Pense em como e onde está a fazer compras online.
- Reconheça os esquemas de phishing: Não clique em ligações nem transfira anexos a menos que tenha certeza da sua proveniência. Confira o endereço de e-mail do remetente e tenha cuidado com solicitações de informações pessoais.
- Nunca forneça a sua palavra-passe, informações pessoais ou financeiras em resposta a um e-mail ou telefonema não solicitado.
- Utilize métodos seguros para as compras: Nunca forneça informações financeiras ao utilizar o Wi-Fi público.
- Utilize um cartão de crédito, quando possível, em vez de um cartão de débito e verifique os extratos de sua conta com frequência.



guide@cyberreadinessinstitute.org

**Retalhistas**

# Esta a época do ano mais movimentada para si, como para os hackers.

Esteja atento aos ataques de ransomware. Em 2020, muitos ataques atingiram empresas conhecidas durante a época festiva dos EUA, um período em que os hackers sabiam que as empresas estariam a esforçar-se por dar vazão às encomendas.

A Sophos Labs estimou que, em 2020, **o setor do retalho foi o mais atingido por ciberataques**. Lembre-se de que os hackers podem tentar passar por si para atingir os seus clientes ou fornecedores.

**Fontes:**


https://www.cisa.gov/news/2021/11/23/cisa-shares-tips-keep-your-personal-data-and-financial-data-safe-holiday-shopping?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202

https://www.politico.com/newsletters/national-security-daily/2021/11/22/chinas-missile-turducken-495192

https://us-cert.cisa.gov/ncas/current-activity/2021/11/22/reminder-critical-infrastructure-stay-vigilant-against-threats

https://www.cisa.gov/news/2021/11/22/cisa-and-fbi-urge-organizations-remain-vigilant-ransomware-and-cyber-threats

https://www.proofpoint.com/us/blog/corporate-news/holiday-shopping-themed-mobile-attacks-increase-dramatically

https://us-cert.cisa.gov/ncas/alerts/aa21-243a

https://www.washingtonpost.com/politics/2021/11/24/happy-hacksgiving-officials-warn-surge-cyber-threats/


## Melhores práticas:

- Identifique os profissionais de tecnologia e cibersegurança que podem responder rapidamente durante a época festiva se ocorrer um incidente cibernético.
- Reforce os avisos à equipa sobre manter a prudência relativamente a e-mails de phishing e outros esquemas cibernéticos durante a época festiva.
- Certifique-se de que os patches de software estão atualizados em todos os dispositivos da empresa e em todos os dispositivos pessoais usados pela sua equipa para realizar o seu trabalho.
- Imponha a utilização de palavras-passe fortes, assegurando que não são reutilizadas em várias contas.
- Certifique-se de que todos os sistemas informáticos exigem aos utilizadores que utilizem a autenticação multifator, especialmente para o acesso remoto e contas administrativas.
- Lembre os seus colaboradores de que não devem clicar em ligações suspeitas e realize exercícios para aumentar a sensibilização.
- Reveja e, se necessário, atualize os planos de comunicação e resposta a incidentes para indicar as ações que uma organização deverá tomar se for afetada por um incidente.
- Certifique-se de que os seus sistemas e dados importantes estão salvaguardados numa cópia de segurança segura guardada num local que não está ligado à sua rede.

## Lembrete:

Se for vítima de um ciberataque, denuncie o incidente à agência de cibersegurança do seu governo, por exemplo: CISA, FBI, Centro Nacional de Cibersegurança do Reino Unido, Interpol.

**Visite becyberready.com, cisa.gov/shop-safely, us-cert.cisa.gov/ncas/alerts/aa21-243a e stopransomware.gov para obter mais informações e conhecer as práticas recomendadas para se manter seguro durante a época festiva.**

CYBER READINESS INSTITUTE