02

SGI INFORMA
MÊS DA SEGURANÇA
DA INFORMAÇÃO
NOVEMBRO - 2020

SGI INFORMA

ESPECIAL - SEGURANÇA DA INFORMAÇÃO

BLACK FRIDAY 2020: CUIDADO PARA NÃO "MORDER" A "ISCA"!

A Black Friday é uma data comercial onde os varejistas adotam a última sexta-feira do mês de novembro para a realização de vendas por meio de ofertas atrativas, levando os consumidores a desfrutarem das vantagens dos altos descontos e a anteciparem suas compras de final de ano.

Em 2020, embora a data oficial seja no dia 27 de novembro, empresários já começaram a antecipar suas promoções para ampliar suas vendas e atrair principalmente o consumidor digital, cujo perfil de compra se dá através da utilização de *e-commerce* e aplicativos mobile.

Onde está o perigo? O perigo está no fato dos cibercriminosos se aproveitarem destas épocas para atraírem usuários desprevenidos, utilizando a técnica de *phishing* para criar promoções e ofertas como iscas para os seus golpes.

Neste período, é comum usuários receberem mensagens via e-mail, aplicativos de mensagens instantâneas, SMS e redes sociais com falsas promoções que aparentam ser de empresas conhecidas, mas que, na verdade, são golpes aplicados com o objetivo de clonar cartões de crédito, roubar informações, emitir boletos falsos, direcionar para sites fraudulentos, instalar software malicioso, dentre outros.

EXPEDIENTE

Secretaria
da Administração - SAEB
Superintendência
de Gestão e Inovação - SGI
Diretoria de Gestão Estratégica
de TIC - DGE
Coordenação de Segurança
da Informação - CSI

Textos: Suane Freitas Coutinho
suane.coutinho@saeb.ba.gov.br

Edição: Ascom/Saeb
ascom@saeb.ba.gov.br

GOVERNO DO ESTADO | SECRETARIA DA ADMINISTRAÇÃO

VOCÊ SABE COMO IDENTIFICAR UMA MENSAGEM DE PHISHING? VAMOS À PRÁTICA!

- **Observe atentamente o endereço completo de e-mail do remetente da mensagem, ainda que exiba o nome de uma empresa confiável. Num e-mail de *phishing*, é comum que o domínio (parte do endereço que fica após o @) seja diferente do endereço da empresa legítima. Caso você identifique isso, suspeite do e-mail e não o abra!**

- **Busque por erros na escrita. Mensagens de *phishing* podem exibir uma quantidade significativa de erros ortográficos e gramaticais. Se isso acontecer, desconfie! Obviamente, espera-se que empresas sérias que têm relação com seus clientes se preocupem em revisar seus textos antes do envio.**

- **Se a mensagem recebida possuir um link, passe o mouse sobre ele e verifique o endereço exibido. Caso seja diferente do endereço de domínio da empresa que aparece como remetente, não clique! Suspeite de golpe! Links suspeitos podem direcionar você para sites fraudulentos que lhe induzem a fornecer dados pessoais ou mesmo a fazer o download de um programa malicioso.**

- **Observe os arquivos que você recebe como anexos, principalmente aqueles de extensão: ".bat", ".jar", ".com", ".cmd", “.msi", ".scr", ".pif", ".reg", ".hta",".js", ".vbs", ".wsf", ".cpl", dentre outros. Tais arquivos podem conter instruções para executar programas com finalidade maliciosa. Desconfie de qualquer anexo desconhecido e não o baixe!**

Não vacile! Seja diligente, não negligente!

SEGURANÇA DA INFORMAÇÃO É VOCÊ QUEM FAZ!

DICAS EXTRAS PARA MINIMIZAR OS RISCOS

1. Desconfie das mensagens com ofertas mirabolantes
As mensagens que chegam por e-mail, SMS e WhatsApp e que induzem ao clique sobre o link com ofertas extravagantes merecem maior atenção. Não clique nem compartilhe tais mensagens com os amigos sem antes verificar a autenticidade.

2. Atenção aos falsos aplicativos
Tenha cuidado ao buscar pelo aplicativo de sua loja preferida, principalmente na hora de aproveitar as promoções. Confira o nome do app e a data de publicação (aplicativos falsos tendem a ter data de publicação mais recente). Outra dica é ir ao site oficial da loja e buscar informações sobre o seu aplicativo para celular.

3. Cuidado com os banners de publicidades enganosas
Falsos banners podem levá-lo a sites maliciosos que visam o roubo de informações ou a distribuição de vírus. Anúncios que nos perseguem em redes sociais ou quaisquer outros sites que visitamos também podem esconder armadilhas e merecem uma maior atenção antes de serem acessados.

4. Atenção na realização de compras on-line
Ao realizar compras on-line, veja se na barra de endereços do navegador é exibido um símbolo de cadeado e o protocolo HTTPS, responsável por promover a comunicação segura entre o seu computador e o site da loja. Não realize transações on-line em lan-houses, cybercafés ou computadores públicos, pois podem não estar protegidos adequadamente.