Domingo, 05 de Abril de 2026

Golpe do abono natalino é nova tática fraudulenta de criminosos

Prática disseminada nos aplicativos de mensagens oferece falsos benefícios em troca de informações pessoais

Novo golpe circula entre aplicativos de mensagens

REPRODUÇÃO/RECORD TV

Um **novo golpe** com a falsa oferta de um **abono natalino** se espalha pelos aplicativos de mensagens **WhatsApp** e Telegram. Entenda a **fraude** e saiba como se proteger.

Segundo a descoberta da empresa especialista em segurança online Kaspersky, com o valor do "benefício" em destaque na tela do site, o golpe se inicia quando a vítima é solicitada a fazer uma consulta na página do abono, ao fornecer nome completo, CPF e data de nascimento.

Após esse envio, a vítima é redirecionada a uma tela para supostamente receber o benefício, com pagamento via Pix. Para isso, ela precisa inserir a chave da conta para que o valor seja enviado.

Em seguida, a pessoa é então levada a mais uma etapa do processo: a disseminação do golpe. Os criminosos solicitam que, para que a vítima receba o benefício, ela envie a "oportunidade" aos contatos no aplicativo. Essa, supostamente, é a última etapa antes do envio do dinheiro.

"Ainda não sabemos a intenção do golpe, uma vez que ele pede para que a vítima envie a página do abono para os contatos, grupos e até no status do WhatsApp. Pode ser que ele instale um malware no aparelho, para roubo de credenciais e dados bancários, ou somente ficar com as informações já fornecidas de CPF e data de nascimento da pessoa. De qualquer forma, é importante estar atento a esse tipo de ataque digital e, sempre que não tiver certeza, não ceder informações pessoais online", comenta Fabio Assolini, diretor da Kaspersky na América Latina.

Para não ser vítima desse tipo de golpe, a companhia recomenda:

1 — Suspeite sempre de links recebidos por e-mails, SMS ou mensagens de WhatsApp, principalmente quando o endereço parecer suspeito ou estranho;

2 — Sempre verifique o endereço do site para onde foi redirecionado, endereço do link e o email do remetente para garantir que são genuínos antes de clicar, além de verificar se o nome do link na mensagem não dirige a outro hiperlink;

3 — Verifique se a notícia é verdadeira acessando o site oficial da empresa ou organização — ou os perfis nas redes sociais;

4 — Se não tiver certeza de que o site da empresa é real e seguro, não insira informações pessoais;

5 — Use soluções de segurança confiáveis para ter uma proteção em tempo real para quaisquer tipos de ameaças.

Fonte: R7