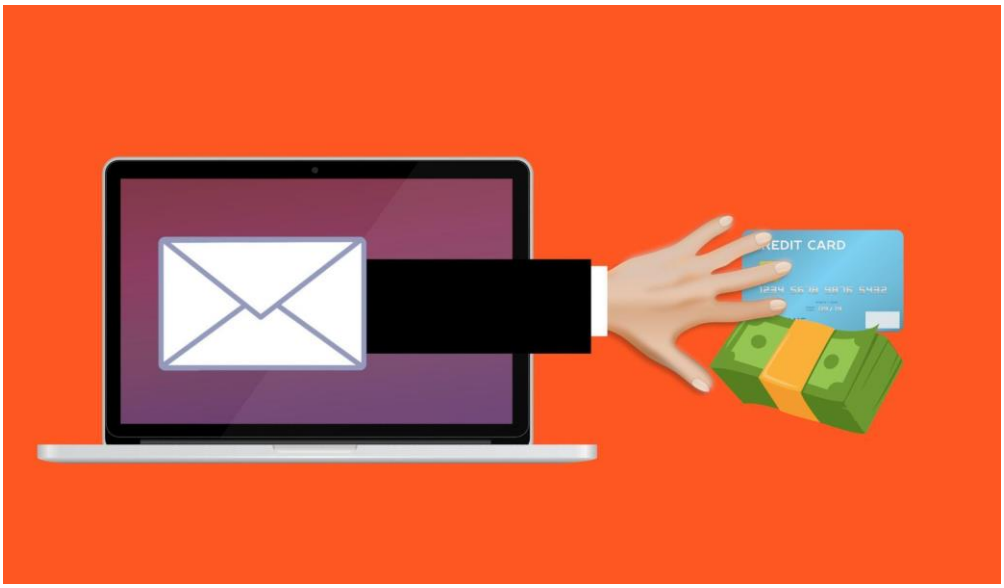
Mês do Cliente: Brasil lidera ranking de vítimas de phishing via WhatsApp, saiba como se prevenir e proteger o consumidor

Getnet lista 6 práticas essenciais para fugir de golpes via e-mail e apps de mensagens



Uma das táticas mais usadas por criminosos digitais, o ***phishing*** é um meio fraudulento para captura de dados confidenciais, como senhas bancárias ou números de documentos pessoais, por exemplo. Conforme dados da Kaspersky, empresa especialista em segurança cibernética, **o Brasil foi o país que mais sofreu com ataques desse tipo pelo WhatsApp no ano de 2022, com mais de 76 mil tentativas de fraudes**, além de ser o quarto país que mais sofreu phishing via e-mail.

Usando canais considerados confiáveis para os usuários, como e-mail ou apps de mensagens instantâneas, os fraudadores enviam às vítimas conteúdos disfarçados, que simulam contatos autênticos, utilizando como pretexto, na maioria das vezes, uma suposta necessidade de atualização de dados ou a entrega de prêmios em dinheiro que o usuário sequer sabia que teria direito.

Ao clicar no link enviado pelo fraudador no conteúdo falso, a vítima é automaticamente direcionada para um site adulterado, também muito similar ao oficial, onde são solicitadas suas senhas e dados pessoais, que então são enviadas diretamente aos criminosos.

Em um ambiente cibernético cada vez mais complexo e desafiador, algumas práticas são essenciais para evitar o phishing, preocupação que é amplificada em datas comemorativas ou comerciais, como o Mês do Cliente, comemorado em setembro, quando o volume de campanhas publicitárias aumenta consideravelmente.

Pensando nisso, **Ricardo Roquette, VP de Tecnologia da Getnet, empresa de tecnologia e soluções de pagamento, do grupo global PagoNxt, do Santander,** separou 6 dicas para qualificar a resiliência cibernética das organizações.

1- **Sempre desconfie, mesmo quando as mensagens forem muito convincentes**

Seja cético com mensagens inesperadas que solicitam informações pessoais ou financeiras, especialmente se elas usam termos com tom de urgência ou ameaçador. Entidades legítimas dificilmente pedirão informações confidenciais por e-mail ou mensagem de texto.

2- **Use URLs e infraestrutura confiáveis e verificadas para acessar gateways**

Gateway é o sistema responsável por conectar e transferir os dados entre usuário e instituição financeira, de forma segura e rápida. Esse sistema é fundamental para que os e-commerces realizem vendas.

Sendo assim, examine quaisquer resultados em navegadores de pesquisa para garantir que o portal de login seja legítimo, evitando confirmação de dados em outros sites, como navegadores de pesquisa, por exemplo.

3- **Verifique cuidadosamente os remetentes**

Mesmo que você receba mensagens de remetentes conhecidos, com relacionamento já estabelecido, como clientes, instituições, órgãos do governo ou lojas, entre outros, certifique-se de que são de fato legítimos antes de clicar em qualquer link ou responder a qualquer mensagem. Preste atenção à ortografia e gramática e verifique se os endereços de e-mail estão corretos.

4- **Não clique em links suspeitos nem faça download de arquivos de fontes não confiáveis**

Se você não tiver certeza se o link recebido é legítimo, digite manualmente o endereço do site na barra de endereço do seu navegador. Assim você consegue identificar qualquer falha no endereço ou reconhecer fontes não confiáveis, evitando ser vítima de phishing.

5- **Mantenha o antivírus e firewall atualizados**

Além disso, execute regularmente uma varredura completa em seu computador ou dispositivo móvel e remova quaisquer arquivos e pastas que não reconheça.

6- **Use senhas complexas e exclusivas para cada conta**

Normalmente, quando precisamos criar uma senha, o próprio site informa a força que ela possui. Opte sempre por senhas fortes compostas por letras maiúsculas, minúsculas, números e símbolos e não as compartilhe com ninguém.

Lembre-se sempre de manter os olhos abertos e tomar as medidas preventivas necessárias para garantir que suas informações pessoais e financeiras sejam seguras e protegidas. Com os ataques de phishing tornando-se uma ameaça persistente, colocando em risco a segurança e a privacidade de indivíduos e organizações, compreender o escopo e o impacto dessas ameaças é crucial para implementar medidas eficazes de segurança cibernética e evitar custos potencialmente prejudiciais.

Sobre a Getnet Brasil

A Getnet é uma empresa de tecnologia para soluções de pagamentos e faz parte da PagoNxt, hub global de meios de pagamentos do grupo Santander. Com mais de 20 anos de atuação, a Getnet Brasil é a terceira maior adquirente do País e oferece um

completo ecossistema de soluções para empreendedores, desde pequenas e médias empresas até grandes companhias. Também é reconhecida como uma das melhores empresas para se trabalhar no Brasil, pelo Great Place to Work (GPTW).

Mais informações em https://getnet.com.br/.

Contatos para a imprensa

Claudia Hercog

claudia@hercogcomunicacao.com.br

Olivia Moderno

olivia@hercogcomunicacao.com.br