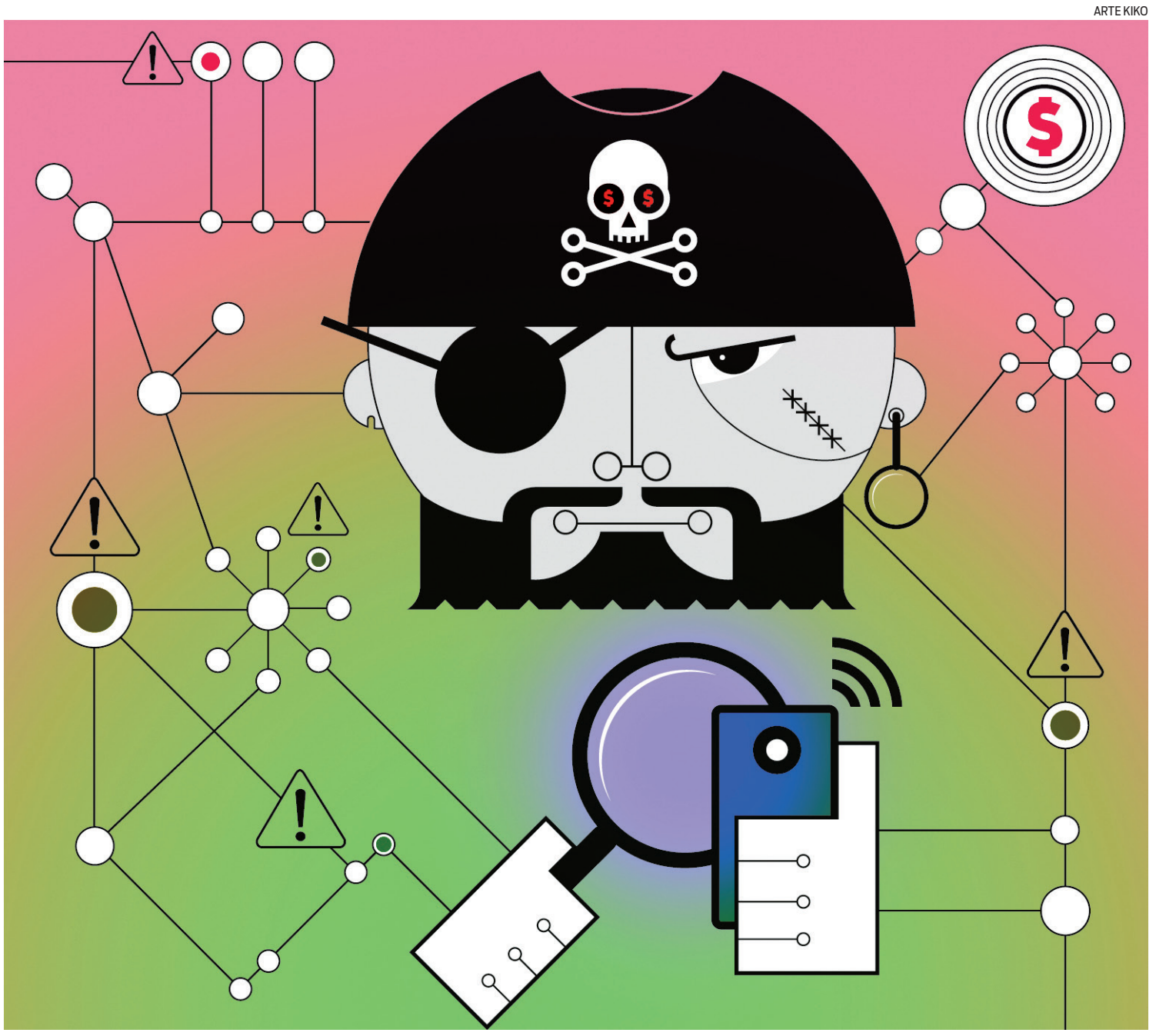
ECONOMIA

BRINDE POR WHATSAPP VIRA ISCA NO DIA DAS CRIANÇAS

Empresa de segurança cibernética alerta para usuário não acreditar nem clicar em ofertas fáceis

MARTHA IMENES
martha.imenes@odia.com.br

ARTE KIKO



O Dia das Crianças chegou e a correria de última hora para comprar presente pode fazer com que o "atrasildo" caia em uma tremenda furada. Os cibercriminosos, aqueles que não têm mais o que fazer que não seja aplicar golpes em pessoas de boa-fé, arrumaram um jeito bem criativo para coletar dados de usuários e gerar tráfego para sites que estão em poder de comparsas. Em menos de 24 horas, segundo a Kaspersky Lab, empresa de cibersegurança, detectou 85 mil acessos a páginas fakes neste período.

Duas "campanhas" maliciosas estão circulando no WhatsApp: uma oferece brinquedo de graça e outra usa como isca os livros da Turma da Mônica. O primeiro golpe se aproveita do nome da loja de brinquedos Ri Happy, prometendo um brinquedo de brinde, caso a URL seja acessada.

Se a vítima clica no link, será direcionada para um site que informa que a empresa varejista reservou 100 mil brinquedos para esta ação e pede para que sejam respondidas três perguntas. Ao respondê-las, o criminoso pede para a vítima compartilhar a mensagem de phishing com dez contatos ou cinco grupos de WhatsApp.

Já a segunda, identificada pela Kaspersky, usa o nome da Turma da Mônica para disseminar o golpe. Essa não é a primeira vez

Para não ser vítima, é importante verificar nos sites oficiais das empresas se a oferta é verdadeira

que isso acontece: no começo do mês um movimento similar usado para roubar dados de cartão de crédito também circulou no aplicativo. Nessa mensagem de phishing, para ganhar o suposto combo de historinhas da marca, a vítima tem que informar dados pessoais como e-mail, número de telefone e nome completo.

VENDA DE DADOS

No primeiro caso, o objetivo da campanha maliciosa é criar tráfego para sites que mostram propaganda. No último, o dano é indireto, já que o site apenas coleta as informações pessoais da vítima. De qualquer maneira, o criminoso irá monetizar os dados ao vendê-los para campanhas de spam ou sendo pago para que ele mesmo realize o disparo da campanha de spam.

"Para evitar ser vítima, é sempre importante verificar sites oficiais das empresas se a oferta é verdadeira. Na dúvida, ligue para centro de atendimento ao cliente para ver se a promoção é verdadeira", destaca Fabio Assolini, analista sênior de segurança da Kaspersky no Brasil.

Empresas negam promoção

> Procurada, a Ri Happy informou ao **DIA** que não faz esse tipo de ação. Em nota, a empresa pede que os clientes sempre verifiquem as promoções vigentes da marca nas próprias lojas físicas ou nos canais oficiais da Ri Happy (Facebook, Instagram e site www.rihappy.com.br). E também pelo telefone 11-3004-2779.

Já a equipe de Maurício de Sousa publicou uma mensagem no Twitter com uma Mônica "boladona" alertando contra o golpe. "A mensagem utiliza indevidamente uma ilustração dos personagens da Turma da Mônica e de sua logomarca com a falsa promessa de presentear com combos de publicações e atividades todo aquele que acessar e se cadastrar em um site indicado e criado pelos autores dessa falsa comunicação".

Tome cuidado com golpe que clona chip do celular

DIVULGAÇÃO

> O uso do celular está em alta, seja para navegar nas redes sociais, fazer compras, acessar e-mail, bater papo do WhatsApp, realizar transações bancárias. Ou seja, tudo está a um simples "touch" do usuário, e é justamente essa praticidade e alcance do celular que chama a atenção dos piratas virtuais, os hackers.

Uma pesquisa divulgada pelo IDC aponta que no Brasil, 65% do total dos entrevistados, entre 18 e 49 anos, usam mais o aplicativo do celular para abrir uma conta bancária ou acessar um produto ou serviço do que ir pessoalmente a uma agência de modelo tradicional (58%).

O celular que facilita a vida do usuário pode ser a porta de entrada para fraudadores. Um dos golpes mais comuns é a clonagem do chip de celular.

Segundo a Kaspersky Lab, quadrilha conseguiu copiar mais de 5 mil chips nos últimos meses, atingindo usuários comuns. Esse golpe dá acesso a contas bancárias e ainda é possível fazer ligações e usar o WhatsApp da vítima.

De acordo com o levantamento, aplicativos de bancos com autenticação via SMS são o grande alvo de criminosos. Ao clonar o número de celular de uma vítima, o criminoso passa a receber todas as ligações e mensagens de texto destinadas a ela.

Com isso, é possível recuperar senhas de apps de bancos tradicionais e digitais, obtendo total acesso ao dinheiro do usuário.

O interesse dos cibercriminosos nas fraudes de SIM swap é tão grande que alguns até vendem este serviço para outros criminosos

FABIO ASSOLINI, da Kaspersky

Segundo a Kaspersky Lab, o grupo teria conseguido fraudar várias contas, gerando prejuízos de até R$ 10 mil para um cliente. Isso acontece porque o processo de obtenção de novo chip para o mesmo número — quando a pessoa perde o aparelho ou tem ele roubado — é falho e criminosos conseguem se passar pelas vítimas.

"O interesse dos cibercriminosos nas fraudes de SIM swap é tão grande que alguns até vendem este serviço para outros criminosos", alerta Fabio Assolini, analista da Kaspersky Lab.

CONFIRA

18 A 49 ANOS

Entrevistados têm entre 18 e 49 anos e usam mais o aplicativo do celular para abrir uma conta bancária ou acessar um produto ou serviço do que ir pessoalmente a uma agência tradicional (58%).

NÃO DÊ BOBEIRA !

WhatsApp também é clonado

■ A técnica de copiar chips também gerou um novo tipo de ataque conhecido como 'clonagem do WhatsApp'. Neste caso, depois da ativação do chip no aparelho do criminoso, ele carrega o WhatsApp para restaurar os chats e contatos da vítima no aplicativo. Então, ele manda mensagens para os contatos como se fosse a vítima, falando de uma emergência e pedindo dinheiro.

E foi exatamente isso que aconteceu com a enfermeira, Renata Lucas, 39 anos, do Rio Comprido. Ela conta ao **DIA** que fez um anúncio de um carro em um site aparentemente confiável e acabou tendo o celular clonado.

"A pessoa me ligou deu todos os dados do carro, número de documentos, e disse que precisava de autenticação para validar meu anúncio e que um link seria enviado por SMS", conta Renata. Ao clicar na mensagem com o link o WhatsApp parou.

"Logo depois disso vários contatos meus começaram a receber mensagens 'minhas' pedindo dinheiro", acrescenta.

Renata entrou em contato com o WhatsApp e pediu que tomassem providências. O número foi bloqueado e em seguida Renata foi orientada a fazer a checagem em duas etapas. E assim foi feito. A preocupação dela foi com os acessos que o golpista teve, inclusive em redes sociais e e-mails.

QUEIXA NA DELEGACIA

A solução encontrada foi dar queixa na delegacia para não ter "surpresas", como falta de dinheiro na conta ou cópia de documentos servindo para fraude. Na Delegacia de Repressão a Crimes de Informática foi aberto um boletim de ocorrência, onde foram anexados os prints das conversas do fraudador com a lista de

Fraudador manda mensagens para os contatos como se fosse a vítima e pede dinheiro.

contatos do telefone clonado e inclusive o número de conta que o golpista forneceu para receber o dinheiro. "Até agora não tive notícia nenhuma", lamenta a enfermeira.

"Embora não haja uma solução milagrosa, a autenticação de dois fatores via SMS é o melhor caminho a seguir. Isso é particularmente verdadeiro quando falamos de Internet Banking. Quando os serviços financeiros pararem de usar esse tipo de autenticação, os golpistas irão focar em outras coisas", diz Fabio Assolini.

Cuidado com autenticação via SMS

> Os usuários devem evitar usar a autenticação de dois fatores via SMS, optando por outros métodos, como a geração de uma autenticação única (OTP) via aplicativo móvel (como o Google Authenticator) ou o uso de um token físico. Infelizmente, alguns serviços online não apresentam alternativas. Nesse caso, o usuário precisa estar ciente dos riscos.

Quando é solicitada a troca do chip, as operadoras devem implementar uma mensagem automatizada que é enviada para o número do celular, alertando o proprietário de que houve uma solicitação de troca do chip e, caso não seja autorizada, o assinante deve entrar em contato com uma linha direta para fraudes.

Isso não impedirá os sequestros, mas avisará o assinante para que ele agir o mais rápido possível em caso de atividades maliciosas. Caso a operadora não ofereça o serviço, o usuário deve entrar em contato solicitando um posicionamento.

Para evitar o sequestro do WhatsApp, os usuários devem ativar a dupla autenticação usando um PIN de seis dígitos no dispositivo, pois isso adiciona uma camada extra de segurança.