Portal do ZACARIAS
Publicado em 10/05/2022 - 08:23

Conheça os golpes mais comuns no WhatsApp e aprenda a se defender

Clonagem de conta e phishing estão entre as principais ameaças aos usuários. Recomendação é sempre desconfiar e não repassar informações.

O WhatsApp está entre os mais populares aplicativos móveis do país, presente em 99% dos smartphones dos brasileiros , segundo a pesquisa Panorama Mobile Time / Opinion Box .

Pela facilidade para troca de mensagens, áudios e arquivos e chamadas por áudio e vídeo, o programa caiu no gosto do povo, mas também dos criminosos. Os golpes na plataforma se multiplicam, exigindo dos usuários cuidados especiais para não se tornarem presas fáceis.

Uma das fraudes mais difundidas é a da clonagem ou sequestro da conta. Criminosos estão aproveitando informações divulgadas em anúncios de sites de classificados para direcionar ataques.

Em posse do nome, telefone de contato e objeto à venda, eles ligam para as vítimas e dizem que o anúncio apresenta problemas. E para liberá-lo, é preciso informar um código recebido por SMS . Esse código, porém, não serve para o site de classificados, mas para a instalação do WhatsApp em outro telefone.

O golpe ficou conhecido e surgiram variantes, seguindo a mesma dinâmica: a busca pelo código SMS . Empresas de segurança cibernética registram casos como o “ golpe da festa ”, no qual os criminosos ligam para a vítima e dizem que elas foram convidadas para uma festa com artistas famosos.

Mas para confirmar a presença, precisam repassar o código recebido por SMS. Existem também ataques direcionados a influenciadores digitais e jornalistas, com falsos convites para eventos de empresas.

"Basicamente, é o mesmo golpe, que está sendo adaptado em outros formatos ", explica Thiago Marques, analista de segurança da Kaspersky. Não existe uma parte técnica, apenas engenharia social. Eles conseguem o contato e procuram

formas de enganar a vítima para terem acesso ao código de instalação do WhatsApp .

Com a posse da conta no WhatsApp , os criminosos podem ter acesso às conversas e aos contatos. A partir daí começa a segunda etapa do golpe: a monetização. Se passando pela vítima, eles enviam mensagens pedindo dinheiro emprestado para familiares e amigos, sempre contando uma história trágica. Não existem estimativas de quantos são os casos e o tamanho do prejuízo, mas pelo aumento no volume de relatos de ataques, a fraude deve ser lucrativa.

"Os atacantes perceberam que isso dá muito dinheiro, porque essas fraudes são cada vez mais comuns" diz Emilio Simoni, diretor do dfndr lab , da PSafe .

A advogada Letícia Marques , do scritório Aith , Badari e Luchin , recomenda que vítimas do golpe entrem em contato imediatamente com o WhatsApp para pedir o bloqueio da conta e avisem seus contatos sobre possíveis pedidos de empréstimos. Além disso, elas devem procurar uma delegacia para registrar um boletim de ocorrência.

"O número de casos está aumentando muito" conta Letícia. "As pessoas chegam desesperadas, sem saber o que fazer.

Para a proteção, a principal recomendação é ativar a verificação em duas etapas, entrando em Configurações > Conta > Confirmação em duas etapas > Ativar . A ferramenta pede que os usuários criem uma senha numérica de seis dígitos, que será exigida na reinstalação do aplicativo. Dessa forma, mesmo em posse do código SMS, os criminosos não conseguirão assumir o controle da conta.

Cuidado com o “phishing”

Outro golpe bastante comum no WhatsApp é o phishing . Nele, os criminosos disparam mensagens em massa, muitas vezes aproveitando temas em alta, para enganar os usuários.

No passado, a fraude era bastante disseminada nos e-mails, mas migrou para os aplicativos de mensagem. Com ofertas irreais, os atacantes conseguem atrair a atenção de desavisados para links falsos, com o intuito de roubar informações ou infectar dispositivos.

A lógica segue a do marketing, de oferecer “promoções” de acordo com a sazonalidade. Com a passagem do carnaval, devem começar a surgir campanhas sobre a Páscoa e o Dia das Mães, com ofertas de chocolate e perfumes, por exemplo. O pânico em torno do coronavírus também deve ser explorado.

Daniel Barbosa , especialista em segurança da informação da ESET , alerta os usuários a desconfiarem de tudo o que recebem, pois os criminosos se aproveitam das próprias vítimas para difundirem o golpe.

"São sempre ofertas maravilhosas, prêmios ou vagas de emprego, que encaminham as vítimas para páginas para o roubo de informações pessoais ou a instalação de malwares. Não acredite se você ganhar uma viagem para Cancún ou perfumes grátis para o presente de Dia das Mães ", diz Barbosa. "E para validar os cadastros, os criminosos pedem que as vítimas repassem a mensagem para seus contatos, para todo mundo viajar junto", completou.

A principal proteção é ativar o desconfiômetro. Tudo que parece bom demais para ser verdade, realmente não é. É golpe. Ao receber mensagens duvidosas, os usuários devem conferir nas páginas oficiais das empresas para atestar a veracidade das informações. Também é recomendável a instalação de softwares de proteção, que impedem o acesso a páginas falsas e a instalação de malwares.

Golpe do crédito

Outra fraude que vem se difundindo no WhatsApp é a do crédito falso . Criminosos enviam mensagens em massa, anunciando a liberação de créditos pré-aprovados em bancos e fintechs. As propostas são tentadoras, com altos valores a juros baixos e condições especiais. Após atrair a vítima, vem o golpe: para ter acesso ao crédito, é preciso antecipar o pagamento de taxas. O pagamento é feito, mas o crédito nunca vem.

"A gente percebeu uma crescente nesse tipo de golpe no ano passado", conta Débora Cippoli , diretora de risco da Noverde , fintech especializada em crédito on-line. — A recomendação é que os clientes que receberem propostas pesquisem se as empresas existem, olhem as páginas oficiais. Abordagem via WhatsApp é incomum entre bancos e fintechs, e o pagamento de antecipação é contra a lógica do crédito. Quem precisa, não tem dinheiro para pagar pela concessão de um empréstimo.

Clonagem do cartão SIM

Um golpe mais elaborado é o da clonagem do cartão SIM . Nele, os atacantes conseguem recadastrar o número de telefone da vítima num outro chip, assumindo o controle num outro smartphone. Pela sofisticação, a técnica não é usada em

ataques em massa, mas para alvos determinados. E com o controle do número de telefone, os criminosos podem facilmente instalar o WhatsApp , já que o código de instalação por SMS será recebido por eles.

Para garantir a proteção do aplicativo, a recomendação é ativar a verificação em duas etapas. Mas nesses casos, o WhatsApp é apenas uma das dores de cabeça para as vítimas. É preciso ativar a dupla autenticação em todos os serviços usados, como e-mails e redes sociais. E após a retomada do número, é preciso alterar todas as senhas.

Ataques cibernéticos direcionados

Pelo WhatsApp também é possível realizar ataques de alta complexidade. Existe a suspeita de que o fundador e diretor executivo da Amazon , Jeff Bezos , tenha tido seu iPhone infectado por um malware por meio de um vídeo enviado pelo aplicativo pelo número do príncipe saudita Mohammed bin Salman .

Segundo análise forense contratada pelo homem mais rico do planeta, um pequeno código implantado no vídeo permitiu a instalação de um programa espião, que deu aos atacantes acesso ao aparelho de Bezos, incluindo suas fotos e comunicações privadas.

Pessoas normais, que não estejam em posições importantes, não precisam se preocupar com ataques com esse grau de sofisticação. O crime cibernético é uma indústria, os atacantes visam nada mais que o lucro, e ações com essa complexidade custam milhões de dólares, muitas vezes para um único uso, já que após a descoberta as vulnerabilidades são corrigidas.

https://portaldozacarias.com.br/site2/noticia/conheaa-os-golpes-mais-comuns-no-whatsapp-e-aprenda-a-se-defender/

Veículo: Online -> Portal -> Portal do Zacarias - Amazonas/AM