Sobre golpes no WhatsApp

Escrito por @o_jovemadulto em 04-09-2021 originalmente aqui.

Não sei na roda de conhecidos de vocês, mas tenho a sensação de que há semanas não passo sem que fique sabendo de alguém que foi vítima de golpes no WhatsApp, seja quando tem seu nome usado para que fraudadores obtenham sucesso, seja enviando, de fato, o dinheiro para o fraudador.

Na data em que escrevo este post duas formas de praticar a fraude se destacam:

1. Quando o sujeito consegue posse do número da vítima e se passa por ela (tecnicamente mais complicado), e
2. quando o fraudador simplesmente usa dados disponíveis e públicos para cometer o crime.

Cada método tem suas peculiaridades, com facilidades, dificuldades e maneiras de se proteger distintas.

Quando você tem seu número furtado.

A fraude mais clássica deste gênero é quando você é supreendido por uma mensagem de um terceiro, muitas vezes se passando por uma empresa ou serviço que te diz enviar um código para confirmar sua identidade.

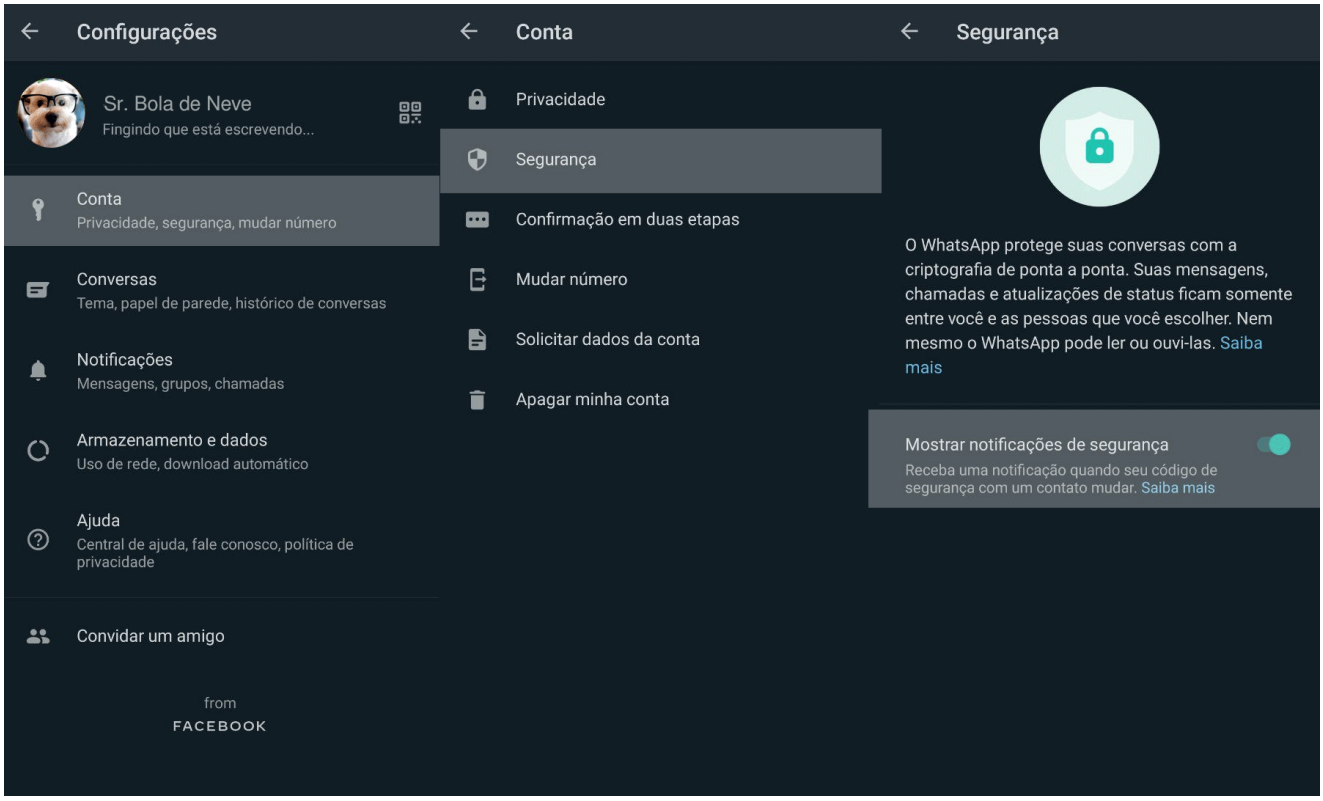
Na verdade se trata do código de confirmação do WhatsApp da vítima, e a a pessoa que comete a fraude está tentando ativar o serviço em seu próprio celular.

Muitas vezes a defesa para esta técnica se resume ao conselho de "ative a proteção de múltiplos fatores". Isso pode ajudar a evitar o problema, mas convenhamos: Se a vítima foi convencida a passar o primeiro código, é relativamente fácil também convencê-la a passar o próximo.

Portanto, **além** de ativar a 2FA (Autenticação de 2 Fatores) vamos ir além!

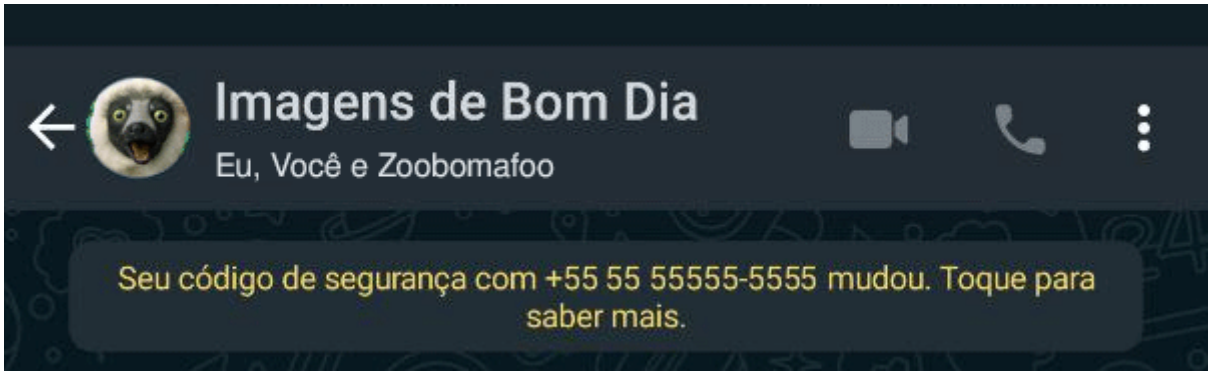
Ative no WhatsApp a função de "Mostrar notificações de segurança" através do caminho: Configurações → Segurança → Mostrar notificações de segurança.

Mais detalhes podem ser encontrados aqui:
https://faq.WhatsApp.com/general/security-and-privacy/security-code-change-notification?lg=pt&lc=BR&eea=0



Explico:
Quando você ativa seu WhatsApp em um dispositivo, é trocado uma informação secreta entre ele e todos os outros com que você mantém contato. Isso inclui grupos, até. É causa/consequência da encriptação Ponta-a-Ponta utilizada.

Com essa opção ativada, você é notificado sempre que uma pessoa com quem você conversa "entra" no WhatsApp por um celular novo.

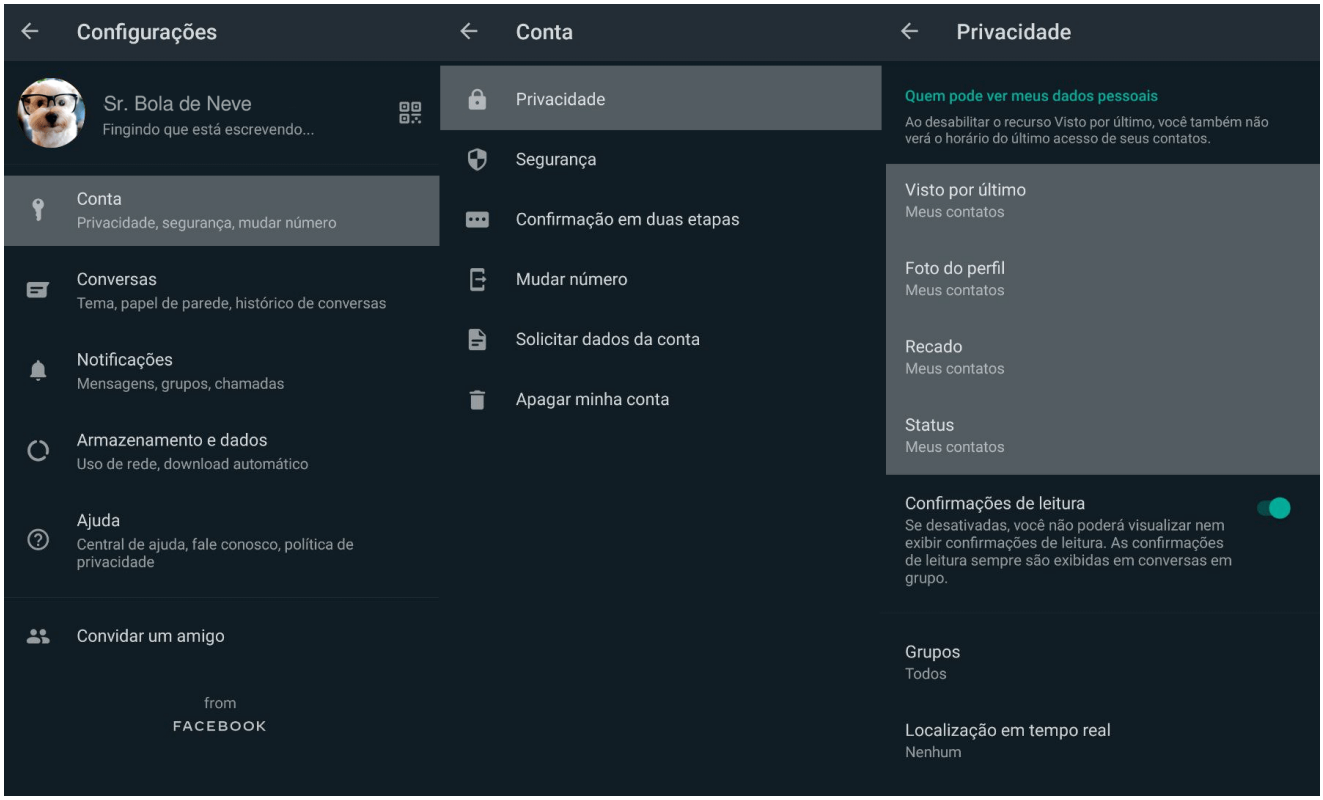


Então já sabe: se aparecer a nota de que "o código do número XX 9XXXX-XXXX mudou" e ele começar a te pedir dinheiro, desconfie (mais do que o normal).

Quando você tem seus dados roubados.

Nesta modalidade não adianta ativar as configurações acima, como ativar as notificações de segurança e o 2FA (faça-os mesmo assim, por favor!). A pessoa do outro lado aborda um familiar ou amigo com um número totalmente novo, mas consegue convencê-los porque copia as imagens de perfil e status da pessoa.

O que devemos fazer neste momento é diminuir as chances de fazer com que a pessoa consiga nossos dados, em primeiro lugar. É só seguir os passos abaixo para que o seu avatar e demais informações não fiquem públicos.



Além disso, vale destacar o perigo de estar em grupos com pessoas desconhecidas (sim, aquele em que você pega as figurinhas também conta) ou compartilhar seu número de telefone com qualquer um.

Lembre-se de que para ser vítima do primeiro golpe basta que tenham o seu número. Para ser vítima do segundo, basta que saibam demais sobre você.

Segurança não é sobre tornar a prática do crime impossível, mas dificultá-la ao máximo. Considere os passos deste post e compartilhe para que seja criada uma rede de segurança ao redor de você e de seus conhecidos.