Polícia Civil do Estado do Rio Grande do Norte

GOLPES DO WHATSAPP

RIO GRANDE DO NORTE
GOVERNO DO ESTADO
SECRETARIA DE ESTADO DA SEGURANÇA PÚBLICA E DA DEFESA SOCIAL – SESED

POLÍCIA CIVIL RN

Golpes do WhatsApp™

Em meio à crescente demanda de crimes virtuais de Estelionato por intermédio do Aplicativo WhatsApp e a ineficácia da evolução dos meios para coibir esta prática, tanto por parte dos desenvolvedores da plataforma e seus dirigentes, quanto pela lei, a melhor maneira de se evitar entrar nessa estatística, que aumenta exponencialmente a cada ano, é a prevenção.

A presente cartilha visa detalhar de forma sucinta os meios mais comuns utilizados pelos estelionatários que utilizam o Aplicativo WhatsApp para aplicar golpes diversos, detalhando, em breve síntese, a forma de agir em cada caso, como o usuário deve proceder caso venha a ser vítima e como se proteger e minimizar os prejuízos ocasionados.

Modalidades:

- Perfil Falso;
- Sequestro de conta para outra linha
- Sequestro da conta (Engenharia Social)

Perfil Falso

Como acontece?

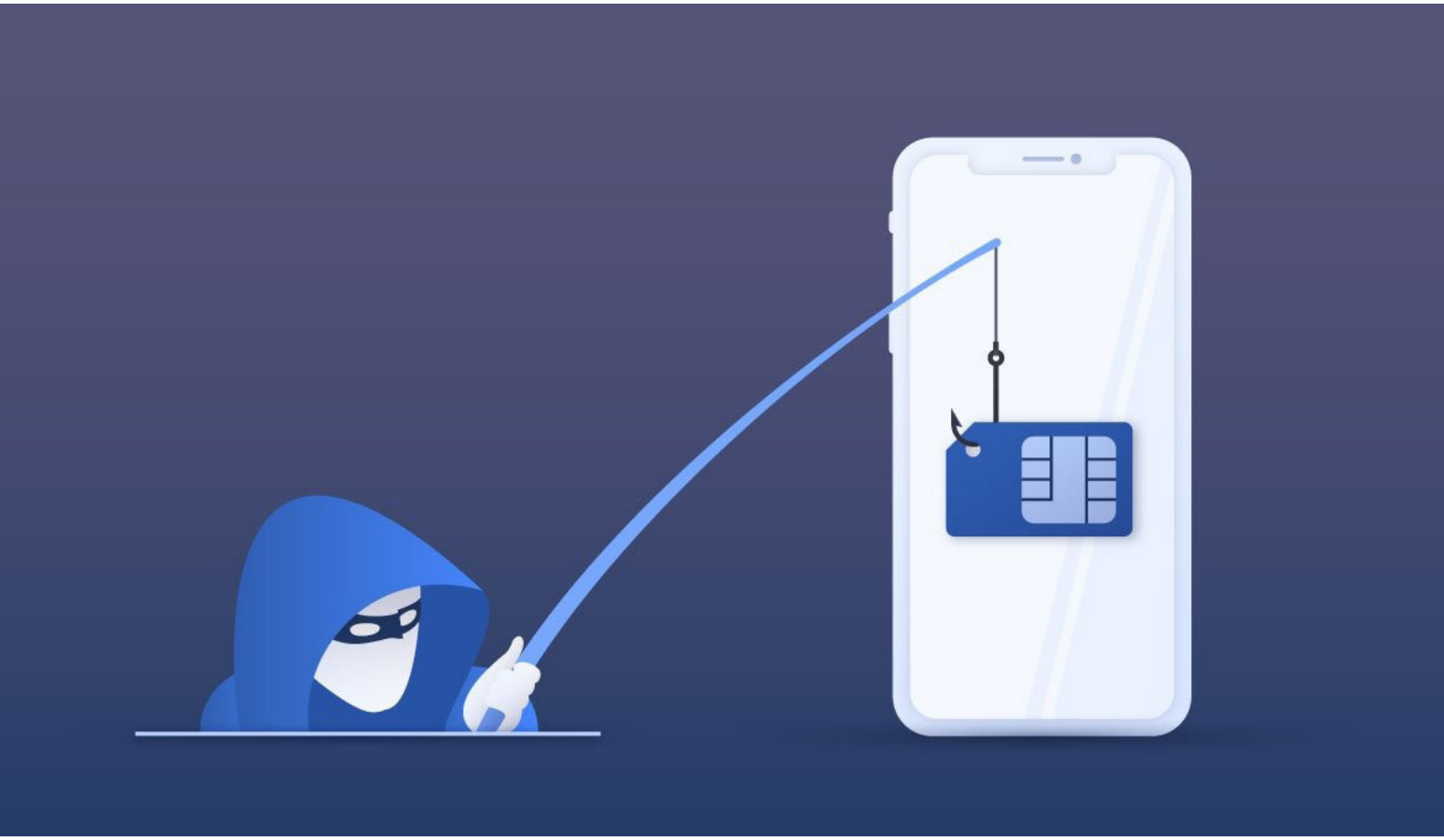
O golpista obtém o número de telefone e outros dados de um usuário do WhatsApp. A partir daí, realiza pesquisas para identificar o nome e o telefone de parentes ou pessoas próximas da vítima, através de consultas em sites clandestinos de fornecimento de dados ou consultas em serviços semelhantes da Deep Web.

Após identificar nomes e telefones de pessoas próximas à vítima, o golpista, utilizando-se de uma linha telefônica qualquer, cria um perfil falso no WhatsApp com a imagem da vítima (obtida em redes sociais ou do próprio perfil original do WhatsApp).

A partir disso, o golpista alega ter trocado de linha telefônica por problemas na conta ou outro motivo e cria uma situação fictícia para solicitar dinheiro emprestado a parentes e amigos da vítima.

O que fazer:

- Desconfie sempre!!! Observe que o golpista usa um numero que não está registrado em seus contatos.
- Entre em contato com o seu parente através do numero que esta salvo em seus contatos e confirme se realmente é ele.
- Crie uma nota de alerta para avisar seus contatos sobre o golpe em suas redes sociais.
- Não deixe evidente contatos de pessoas próximas e familiares ao registrá-los! Se o golpista obtiver acesso à sua lista de contatos por algum meio, pesquisará inicialmente por entradas cadastradas como “Mãe”, “Tia”, “Amor” etc.
- Configure o App WhatsApp para que suas informações de perfil somente sejam exibidas para contatos registrados - Configurações > Conta > Privacidade > Foto do Perfil e marque “Meus Contatos”.
- Envie um e-mail para: support@whatsapp.com com o assunto: URGENTE - PERFIL FAKE informando o número de telefone que está se passando por você no formato DDI+DDD+LINHA, ex: +55 (84) 96555-0101.
- Registre um Boletim de Ocorrência.



SEQUESTRO DE CONTA WPP PARA OUTRA LINHA TELEFÔNICA (SIMSWAP)

Como acontece?

O golpista, utilizando-se de documentos falsos em nome do usuário do aplicativo WhatsApp, comparece, de forma presencial, em postos de atendimento das empresas de telefonia celular ou por meio da participação direta de pessoas que prestam serviços para tais empresas e transfere a linha telefônica do usuário do aplicativo para outro chip (SimCard), dessa forma o usuário vítima perde imediatamente o acesso ao aplicativo e à sua linha telefônica.

Após a transferência da linha telefônica, o golpista faz a instalação do aplicativo WhatsApp no telefone que está em seu poder. A partir disso, o golpista se passa pela vítima e, alegando problemas na conta ou com o cartão bloqueado, cria uma situação fictícia para solicitar dinheiro emprestado a parentes e amigos da vítima.

O que fazer:

- Envie e-mail para support@whatsapp.com informando o número do telefone vinculado ao aplicativo WhatsApp (exemplo de número de celular do Brasil: +55 61 95265-XXXX) solicitando a imediata desativação da conta em razão de fraude.

Como se proteger:

- Sempre desconfie!
- Habilitar a “confirmação em duas etapas”– no ”WhatsApp” clicar em “Configurações > Ajustes”, depois clicar em “Conta” e depois em “confirmação em duas etapas”.

Como recuperar a linha:

Compareça a um posto de atendimento de sua operadora telefônica para relatar que sua linha foi transferida para outro chip (sim card) sem sua autorização e solicitar o imediato restabelecimento da linha.

SEQUESTRO DA CONTA (ENGENHARIA SOCIAL)

Como acontece?

O golpista utiliza técnicas de engenharia social para convencer o usuário a passar os códigos SMS de recuperação da conta sob o pretexto de receber alguma oferta ou bonificação. De posse do código, habilita a conta WPP da vítima em outro aparelho celular e se passando por ela, solicita transferência de valores dos contatos para conta bancária de terceiros.

O que fazer:

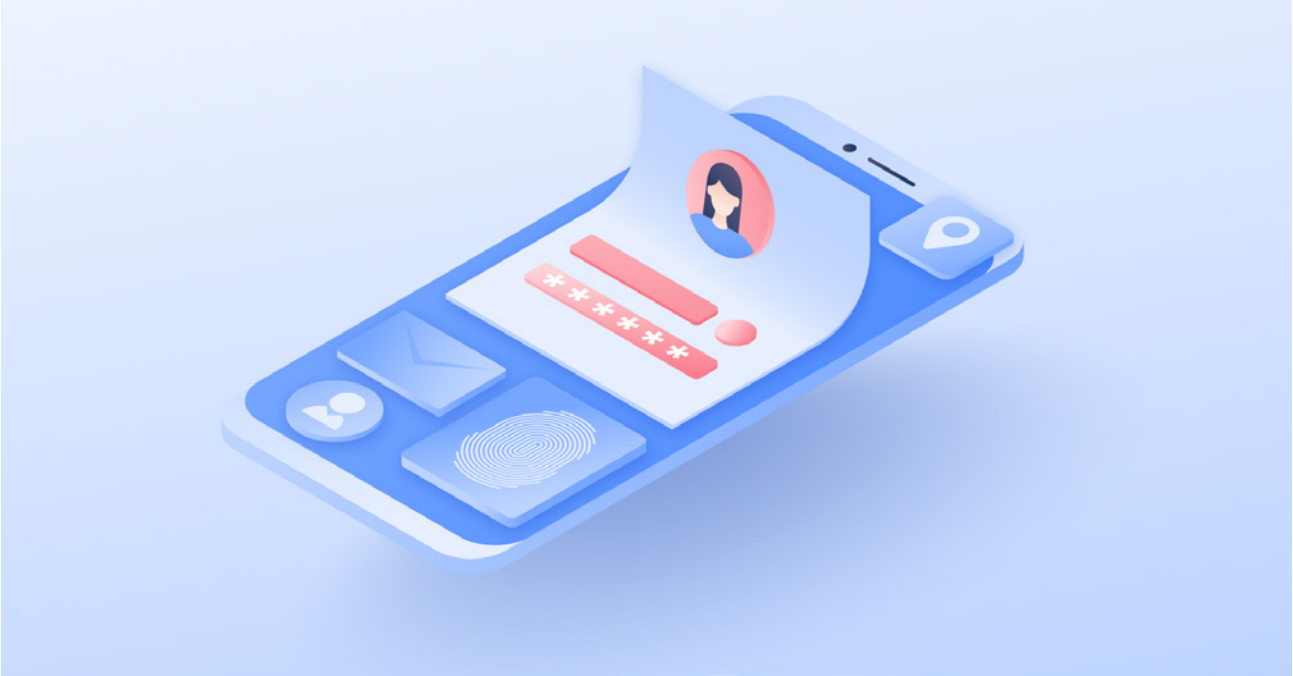
- Avise familiares e contatos.
- Envie e-mail para support@whatsapp.com informando o número do telefone vinculado ao aplicativo WhatsApp (exemplo de número de celular do Brasil: +55 61 95265-XXXX) e solicitando a imediata desativação da conta em razão de fraude.
- Habilite a verificação em duas etapas.
- Não registre contatos de familiares com nome que os identifique (Mãe, Tia, Amor etc.).
- Registre um Boletim de Ocorrência.

Como evitar:

Para que este método de golpe se perpetue, o golpista precisa ter acesso ao código SMS que é enviado ao usuário quando este solicita a recuperação da conta. Portanto:

- Não forneça, transmita ou confirme seus dados pessoais para contatos desconhecidos sob qualquer pretexto;
- Os álibis mais comuns utilizados são: Hospedagens gratuitas; Festa Vip; Auxílio Emergencial; Atualização cadastral em plataformas de comércio eletrônico (OLX, Mercado Livre); Sites de venda de imóveis; Descontos em supermercados e restaurantes; SMS por engano com solicitação de envio para terceiro.

DISPOSIÇÕES FINAIS:



Caso venha a ser vítima, procure imediatamente a Delegacia do seu bairro em horário comercial ou a Delegacia de Plantão para registrar um Boletim de Ocorrência;

No Boletim, informe dia e hora em que ocorreu o fato com a descrição do problema, a forma como ocorreu, o período no qual ficou sem acesso ao telefone e aplicativo e o número utilizado pelo infrator e vítima;

Tome nota ou print das Contas bancárias e chaves PIX utilizadas no golpe, comprovantes e identificação das vítimas e de valores depositados para complementar o Boletim;

Entre em contato com sua instituição financeira para relatar o fato e informar que a conta do infrator está sendo utilizada para aplicação de golpes e verifique se há opções de ressarcimento para o seu caso.

Nos casos que envolvem o SIMSWAP, há a responsabilidade das Operadoras sobre a guarda dos dados cadastrais dos usuários, portanto, gera-se o direito de acionar judicialmente a operadora de telefonia por falha na prestação do serviço - Art. 14 do CDC.

SOBRE O PIX

Importante

Em novembro de 2021, o PIX recebeu dois procedimentos no intuito de coibir as fraudes que se beneficiam com a praticidade deste meio de transferência, sendo eles o “Bloqueio Cautelar” e o “Mecanismo Especial de Devolução”;

As duas medidas atuam em conjunto e podem bloquear a conta de destino, utilizada para transferências fraudulentas, e assim possibilitar a devolução dos valores após prévia auditoria;

Para a eficácia das medidas, a vítima precisa agir rápido e as instituições financeiras exigem o registro prévio de Boletim de Ocorrência Policial;

Se informe na íntegra no site: https://www.bcb.gov.br/detalhenoticia/591/noticia

Registre seu Boletim online no site:
https://www3.defesasocial.rn.gov.br/BoletimCidadao/index.jsf


POLÍCIA
CIVIL
RN