E-BOOK

guia de segurança

Lembrete

Segurança em primeiro lugar, a Xiaomi cuida de você

Tecnologia de qualidade
acessível para todos.

ÍNDICE

Tecnologia de qualidade
acessível para todos.

1. CLONAGEM DE WHATSAPP

1.1. O golpe ocorre da seguinte forma:

O criminoso liga ou envia uma mensagem se passando por um funcionário de um site de compra ou de um banco e diz que estará encaminhando um código promocional ou código de confirmação. Ele pede para que a vítima informe esse código, que na verdade é a verificação do WhatsApp. Com esse código, o criminoso consegue clonar a conta do consumidor. Após a clonagem, o criminoso passa a enviar mensagens para os contatos da vítima, se passando por ela e pedindo dinheiro. As desculpas para solicitar dinheiro emprestado são as mais diversas, e na maioria das vezes, os alvos principais da investida são os parentes mais próximos e amigos que, acreditando na mensagem, acabam depositando ou transferindo valores seguindo as coordenadas do criminoso.

1.2. Como evitar o golpe:

a) Ative a "Confirmação em duas etapas" no WhatsApp. Acesse o link e veja como: https://faq.whatsapp.com/1278661612895630/?locale=pt_BR
b) NUNCA forneça o código verificador que você recebe via SMS em seu celular.
c) Não instale apps de terceiros ou compartilhe informações pessoais a pedido de ninguém pelo whatsapp.
d) Desconfie de situações em que a pessoa solicita a realização de transferências e pagamentos em caráter de urgência.
e) Ligue para a pessoa que solicitou o dinheiro e verifique se realmente é ela quem está solicitando a transação.

1.3. Caso tenha sido vítima, o que fazer:

1.3.1. Vítima do celular clonado

a) Envie um e-mail para support@whatsapp.com com o assunto "CONTA HACKEADA – DESATIVAÇÃO DE CONTA". Relate o ocorrido e siga as instruções do provedor.
b) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home na opção OUTROS CRIMES.
c) Peça para amigos e familiares excluírem o telefone clonado de grupos e alertarem o máximo de contatos em comum sobre o ocorrido.

1.3.2. Vítima foi quem fez o pagamento

a) Entre em contato com o banco e tente bloquear o valor.

b) Providencie cópia (prints) das conversas realizadas, bem como do comprovante de pagamento.

c) Em posse dessas informações, procure uma Delegacia de Polícia para o registro de Boletim de Ocorrência.

2. GOLPES ENVOLVENDO PIX

2.1 Recomendações

As recomendações em relação às transações PIX são, em geral, as mesmas para proteger o acesso a serviços financeiros já utilizados, como TED e DOC. Não acesse sites desconhecidos ou instale aplicativos desconhecidos no celular. Não existem sites ou aplicativos do Banco Central ou do Pix criados exclusivamente para cadastrar as chaves ou realizar transações Pix. O cadastramento das chaves é feito em ambiente logado no aplicativo ou site da sua instituição financeira, o mesmo utilizado para outras transações, como consultar saldo, fazer transferências ou obter empréstimos. O cadastramento das chaves requer o consentimento do cliente e envolve uma validação em duas etapas. O cadastro do número de celular ou e-mail como chave Pix exige confirmação por meio de um código enviado, por exemplo, por SMS ou para o e-mail fornecido. Já o CPF/CNPJ só pode ser usado como chave se estiver vinculado à conta, informação necessária no momento da abertura da conta, comprovada por meio de documento. Se tiver dúvidas, procure informações no site da sua instituição financeira. Não há prazo para cadastrar as chaves, o processo estará sempre disponível.

2.2 Caso tenha sido vítima, o que fazer:

a) Reunir toda documentação da transação (extratos, comprovantes, etc)

b) Registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica: https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home na opção OUTROS CRIMES ou registre os fatos presencialmente no Distrito Policial mais próximo da residência.

c) Cientificar o prestador de serviço de pagamento para eventual ressarcimento, após análise dos documentos.

3. “RANSONWARE” (SEQUESTRO DE DADOS)

3.1. O golpe ocorre da seguinte forma:

O ransomware é um vírus que “tranca” os seus dados até o pagamento de um resgate.

Na maioria das vezes à invasão ocorre no período da noite ou madrugada, momento em que um criminoso virtual invade o dispositivo da vítima e instala um software capaz de criptografar (codificar) as informaçoes de seu computador. Ao acessar o computador após tal procedimento, a vítima receberá uma mensagem de que seus dados foram criptografados e se ela não realizar um pagamento exigido pelo criminoso, normalmente em bitcoins, a vítima perderá todos os dados do computador invadido.

3.2. Como evitar o golpe:

a) Mantenha backup atualizado do computador, de preferência em HD externo ou pen drive e nunca os deixe espetados no computador, pois também poderão ser invadidos ou infectados;

b) Mantenha antivírus e firewalls sempre ativados e atualizados;

c) Evite acesso a sites suspeitos;

d) Não clique em links duvidosos de e-mails suspeitos.

3.3. Caso tenha sido vítima, o que fazer:

a) Não apague os e-mails e/ou mensagens recebidas do criminoso;

b) Se houver conversa com o criminoso via rede social, salve o nome do perfil e o link completo do perfil (endereço completo que aparece ao se clicar na barra de endereço);

c) Em caso de contato por telefone, faça uma relação todos os números de telefone utilizados pelo criminoso, contendo data e horário das conversas;

d) Anote os dados de eventuais contas bancárias, inclusive carteiras eletrônicas de bitcoins informados pelo criminoso;

e) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica **https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home** **na opção OUTROS CRIMES.**

4. Sites de comércio eletrônico fraudulentos

Prática criminosa que tem como alvo clientes de sites de comércio eletrônico.

4.1. O golpe ocorre da seguinte forma:

Nessa modalidade, o golpista cria uma página na internet muito semelhante à verdadeira, levando a vítima a acreditar que está efetuando uma compra legítima. Após selecionar os produtos e efetuar o pagamento, a vítima não recebe a mercadoria, quando então percebe que "caiu em um golpe".
Para aumentar as chances de sucesso, o estelionatário utiliza artifícios, tais como: envio de spams, oferta de produtos com valor abaixo do valor de mercado, propagandas através de links patrocinados, dentre outros.
Além do comprador, as empresas que tiveram seus nomes utilizados indevidamente, ou ainda, as pessoas que tiveram seus dados utilizados para criação do site ou para a abertura de "empresas fantasmas", também são vítimas.

4.2. Como evitar o golpe:

Algumas dicas são indispensáveis, para que possamos ter a certeza que estamos fazendo uma compra legítima, com segurança:
a) Procure utilizar terminais (computador, smartphone, tablet) que sejam seguros;
b) Leia atentamente as informações dos sites e do produto que deseja comprar. Normalmente, sites fraudulentos podem conter erros de português ou ainda sobre as informações técnicas do produto. Verifique também se há CNJP cadastrado na página ou canais de comunicação;
c) Faça uma pesquisa de mercado do valor do produto que deseja adquirir. Desconfie de preços muito baixos;
d) Realize pesquisas na internet para obter informações a respeito da reputação do site em que deseja efetuar compras. Essas informações podem ser obtidas através do Reclame Aqui ou de redes sociais. É possível ainda verificar a lista de sites reprovados, disponibilizada pelo Procon **(https://www.procon.sp.gov.br)**
e) Verifique se o site é seguro, localizando o ícone de um cadeado, ao lado do endereço do site (URL). Ao clicar no cadeado, será exibido o certificado de segurança da página;
f) Evite clicar em links que direcionam a navegação diretamente ao site de compras. Ao invés disso, prefira digitar o endereço do site (URL) junto à barra de endereço de seu navegador. Atenção: os sites fraudulentos geralmente possuem o endereço muito semelhante ao site verdadeiro. Exemplo: www.americanas.com.br (site verdadeiro) e www.lojasamercanas.com.br (site falso – exemplo fictício).

Note que no exemplo do site falso foi incluído o nome “lojas” e a letra “i” do nome “americanas” foi suprimida.
Sites de comércio eletrônico fraudulentos

4.3. Caso tenha sido vítima, o que fazer:

a) Verifique se o site ainda está ativo e copie seu endereço (URL);

b) Faça um print da página e do produto anunciado;

c) Providencie uma cópia do boleto ou dados bancários utilizados para o pagamento, bem como do comprovante do pagamento;

d) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou rregistre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica **https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de- cidadao/home** na opção **OUTROS CRIMES**.

5. FRAUDES BANCÁRIAS: FALSO FUNCIONÁRIO OU FALSA CENTRAL DE ATENDIMENTO:

O fraudador se passa por um funcionário do banco e alega problemas no cadastro ou irregularidades na conta da vítima. A vítima, acreditando na história, acaba fornecendo informações sobre sua conta, permitindo que o criminoso realize transações fraudulentas.

a) Falso motoboy: Membros de uma quadrilha entram em contato com a vítima, fingindo pertencer ao centro de relacionamento do banco. Eles afirmam que houve problemas com o cartão da vítima e solicitam que ela digite sua senha numérica no teclado do telefone. Em seguida, afirmam que enviaram um motoboy à casa da vítima para pegar o cartão. Com o cartão e a senha em mãos, eles realizam operações fraudulentas.

b) Phishing: O criminoso envia links, e-mails e mensagens de SMS para a vítima, geralmente explorando emoções como curiosidade, medo ou prometendo uma oportunidade única. Essas mensagens enganam a vítima, levando-a a clicar nos links ou abrir anexos que roubam dados pessoais ou a induzem a fornecer informações ou se cadastrar em serviços fraudulentos.

5.1. Como evitar o golpe:

a) Evite usar computadores públicos e redes abertas de wi-fi para acessar conta bancária ou fazer compras online.

b) NUNCA abra e-mails de origem ou de procedência duvidosa.

c) Não execute programas, abra arquivos ou clique em links que estejam anexados ou no corpo desses e-mails.

d) Delete esses e-mails e, caso tenha clicado em alguma parte deste e-mail e executado um programa, comunique imediatamente ao seu banco o ocorrido e altere todas as suas senhas de acesso à sua conta bancária em outro computador confiável, ou no mesmo, após uma verificação completa de infecção de vírus por um técnico confiável;

e) NUNCA utilize seu cartão para fazer compras em sites desconhecidos.

5.2. Caso tenha sido vítima, o que fazer:

a) Entre em contato com o banco e tente bloquear o valor.

b) Tire cópia do comprovante de pagamento e demais documentos correlatos.

c) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao home na opção OUTROS CRIMES.

A XIAOMI CUIDA DE VOCÊ

Tecnologia de qualidade
acessível para todos.