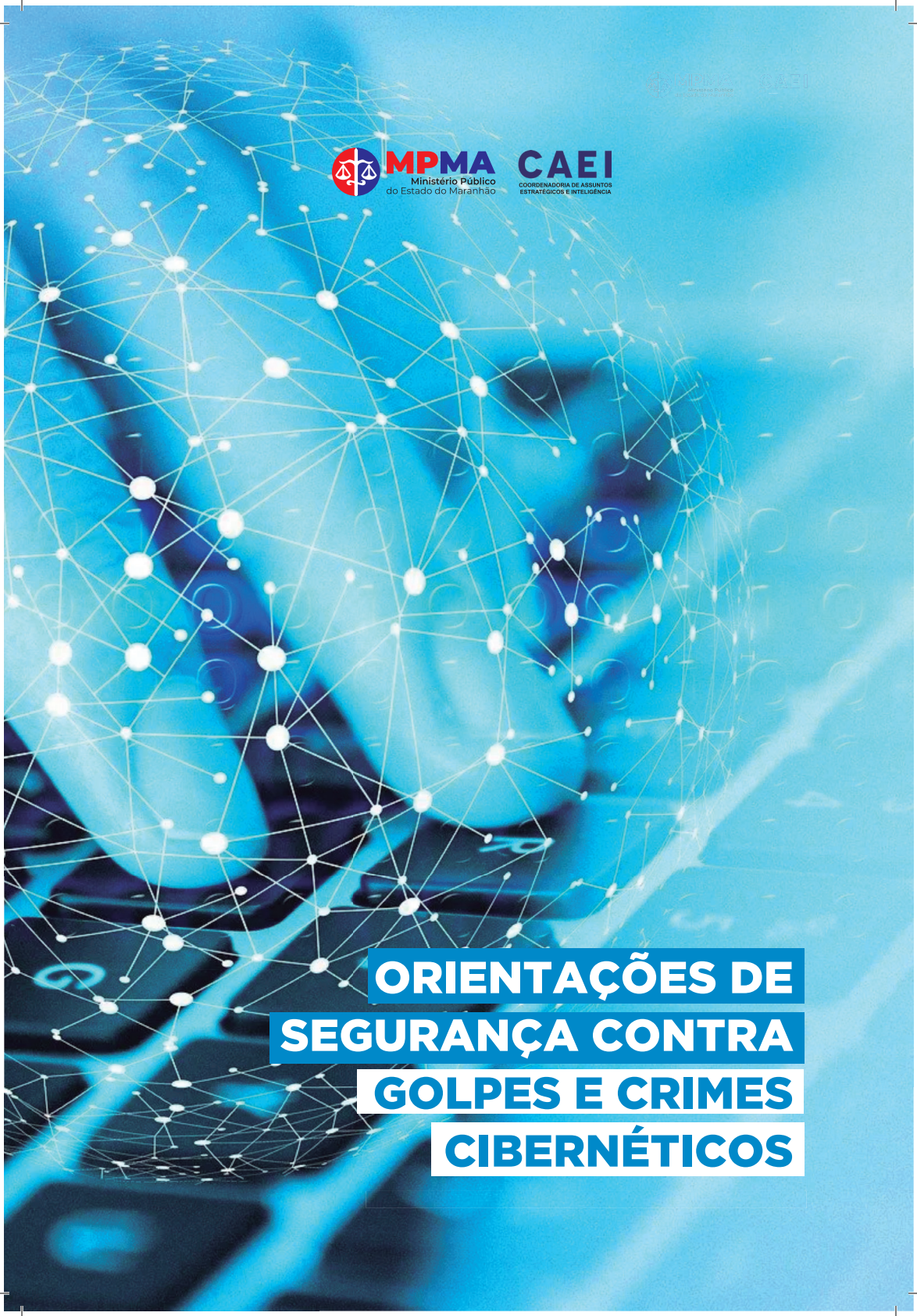
MPMA
Ministério Público
do Estado do Maranhão
CAEI
COORDENADORIA DE ASSUNTOS
ESTRATÉGICOS E INTELIGÊNCIA
ORIENTAÇÕES DE
SEGURANÇA CONTRA
GOLPES E CRIMES
CIBERNÉTICOS

MPMA Ministério Público do Estado do Maranhão

CAEI COORDENADORIA DE ASSUNTOS ESTRATÉGICOS E INTELIGÊNCIA

ORIENTAÇÕES DE SEGURANÇA CONTRA GOLPES E CRIMES CIBERNÉTICOS

PROCURADORIA GERAL DE JUSTIÇA DO ESTADO DO MARANHÃO

EDUARDO JORGE HILUY NICOLAU
Procurador-Geral de Justiça

DANILO JOSÉ DE CASTRO FERREIRA
Subprocurador-Geral de Justiça para Assuntos Jurídicos

REGINA MARIA DA COSTA LEITE
Subprocuradora-Geral de Justiça para Assuntos Administrativos

THEMIS MARIA PACHECO DE CARVALHO
Corregedora-Geral do Ministério Público

SANDRA LÚCIA MENDES ALVES ELOUF
Ouvidora do Ministério Público

JÚLIO CESAR GUIMARÃES
Diretor-Geral da PGJ

JOSÉ MÁRCIO MAIA ALVES
Diretor da Secretaria para Assuntos Institucionais

EDNARG FERNANDES MARQUES
Diretor da Secretaria de Planejamento e Gestão

THERESA MARIA MUNIZ RIBEIRO DE LA IGLESIA
Chefe de Gabinete do PGJ

Coordenadoria de Assuntos Estratégicos e Inteligência

PAULO ROBERTO SALDANHA RIBEIRO
Presidente da Comissão de Segurança Institucional

LUIZ MUNIZ ROCHA FILHO
Coordenador de Assuntos Estratégicos e Inteligência

MAJOR QOPM REGINA CLAUDIA DOS SANTOS GOMES
Chefe da Seção de Segurança Institucional-PGJ

Procuradoria Geral de Justiça do Estado do Maranhão - Sede
Av. Prof. Carlos Cunha, nº. 3261, Calhau. São Luís-MA
CEP: 65076-820 - Fones: (98) 3219-1600 / 3219-1624
Homepage: http://www.mpma.mp.br

Centro Cultural e Administrativo do Ministério Público do Maranhão
Rua Osvaldo Cruz, 1396 - Centro. São Luís-MA
CEP: 65020-910 - Fone: (98) 3219-1804 / 1980
Homepage: http://www.mpma.mp.br

ORIENTAÇÕES DE SEGURANÇA CONTRA GOLPES E CRIMES CIBERNÉTICOS

Editoração Eletrônica e Capa
Renê da Silva Caldas

Sumário

Apresentação

A utilização da tecnologia como ferramenta para realização de tarefas cotidianas e profissionais de forma prática e ágil, vem se tornando habitual e necessária nos dias atuais.

Por meio da internet, várias atividades e ações foram simplificadas e possibilitadas de serem executadas de forma virtual, sem a necessidade de comparecimento em espaço físico, desde o uso de aplicativos para a compra de alimentos e medicamentos, bem como a sua utilização para participações em cursos, palestras, eventos, realização de trabalho remoto, movimentações bancárias, entre outras tarefas.

Porém, apesar dessa praticidade, o ambiente virtual para muitas pessoas ainda é um mundo completamente novo, onde não há conhecimento suficiente para a realização dos procedimentos mínimos de proteção de seus dados pessoais, tornando-se, portanto, vítimas fáceis para criminosos e golpistas.

Nesse sentido, a Coordenadoria de Assuntos Estratégicos e Inteligência, por meio da Seção de Segurança Institucional, preocupada com seus principais ativos dentro da instituição ministerial, vem por meio deste material fornecer orientações e alertas para que Membros e Servidores do Ministério Público do Estado Maranhão, possam se proteger de crimes cibernéticos e adotar medidas preventivas contra possíveis golpes virtuais.

1. Golpe dos falsos links

Neste tipo de golpe os criminosos, por meio de mensagens, afirmam que a vítima foi sorteada em alguma promoção, ou enquadra-se para algum tipo de benefício ou ainda que teria ocorrido alguma operação indevida na sua conta.

Os criminosos, então, dizem que para o recebimento dos benefícios ou solução do problema faz-se necessário acessar um link que foi enviado por mensagem.

Após acessar o link a vítima é redirecionada para sites falsos de cadastro ou então baixa automaticamente aplicativos maliciosos, com o objetivo de obter informações pessoais.

Orientações:

Sempre desconfie de links encaminhados por mensagens via Whatsapp e/ou SMS, e na dúvida, entre em contato pelos canais oficias de atendimento ao consumidor;

O que fazer se cair neste golpe?

- Caso tenha acessado o link e realizado o cadastro informe ao seu banco, e procure assistência especializada para verificação da presença de aplicativos maliciosos no seu aparelho;
- Registre um boletim de ocorrência junto a Polícia Civil, mencionando o número do telefone utilizado para envio do link falso.

2. Golpe da troca de cartão

Os criminosos entram em contato com a vítima se passando pela instituição financeira do cartão de crédito e alegam que houve uma compra duvidosa. Em virtude disto, solicitam que a vítima entre em contato pelo número indicado no verso do cartão para efetuar o seu cancelamento tentando passar credibilidade à farsa.

Mas o golpista não desliga o telefone e coloca uma música similar às utilizadas por empresas de telemarketing, solicitando, após algum tempo, informações sobre a vítima e sobre o cartão. A vítima, se estiver desatenta, sem perceber repassa informações sensíveis.

Na sequência, o golpista informa que um funcionário da instituição irá até à residência da vítima para efetuar a troca do cartão. De posse do cartão, os criminosos podem efetuar compras e pagamentos.

Orientações:

Nunca forneça seus dados pessoais ou bancários via telefone;

- Caso receba ligações de instituições financeiras, dirija-se à agência bancária para confirmar a informação;
- Na impossibilidade de se dirigir até uma agência, encerre a ligação, espere alguns minutos e entre em contato pelos canais oficiais de atendimento do estabelecimento bancário.

O que fazer se cair neste golpe?

- Entrar em contato com a Instituição Bancária solicitando o cancelamento do cartão;
- Registrar um boletim de ocorrências junto a Polícia Civil mencionando o número do telefone utilizado pelo golpista, bem como qualquer informação que possa ajudar na identificação da pessoa que buscou o cartão na sua residência;

3. Golpe de clonagem de perfil no Whatsapp

Neste golpe os criminosos conseguem o número de telefone das vítimas, geralmente, em anúncios postados em plataformas de compra e venda ou em anúncios públicos nas redes sociais.

De posse do número da vítima os criminosos se passam por funcionários das plataformas ou de alguma outra empresa, e por meio de diversos pretextos, solicitam os dados pessoais e o código de 6 dígitos que a vítima receberá no telefone.

Esse código de 6 dígitos, na realidade, é uma verificação do Whatsapp. De posse dessa chave de verificação os golpistas poderão desviar o whatsapp da vítima para outro aparelho, e esta perderá o acesso ao seu whatsapp. Com o controle do whatsapp os criminosos passam a solicitar quantias em dinheiro para a lista de contatos, gerando novas vítimas do golpe.

Orientações:

Jamais compartilhe com terceiros o código de seis dígitos do *Whatsapp* enviado via SMS, para evitar que criminosos tenham acesso a sua conta;

- Redefina a configuração de segurança da sua conta do *Whatsapp* para confirmação em duas etapas;
- Na hipótese de entrarem em contato com você para resolver um problema financeiro, fale diretamente com a empresa pelo Serviço de Atendimento ao Consumidor – SAC, pois, empresas como OLX, Mercado Livre, entre outras, não solicitam códigos de confirmações para aprovação de anúncios;
- Desconfie de mensagens solicitando depósitos e transferências bancárias;
- Se algum contato de sua agenda telefônica lhe solicitar dinheiro, fale com essa pessoa por telefone ou pessoalmente para confirmar se de fato é a pessoa que está solicitando esse repasse financeiro;

O que fazer se cair neste golpe?

Se você foi vítima do golpe de clonagem de perfis no *whatsapp*, faça os *prints* da conversa com o golpista e, imediatamente, envie para o suporte técnico do whatsapp (support@whatsapp.com) descrevendo no cabeçalho do e-mail " Perfil Fake- Desativar Conta", informe o número do telefone que aparece no perfil *fake*, mencione o número do seu telefone, colocando o código +55 (DDD) antes do número do telefone, no corpo da mensagem relate o problema anexando cópia dos prints e se possível, envie a cópia do seu RG;

Denuncie o número utilizado pelos golpistas entrando no campo “dados do contato” e clicando em “denunciar”;

- Registre um boletim de ocorrência junto a Polícia Civil, mencionando o número do telefone utilizado pelo golpista;
- Alerte também, o mais rápido possível, os seus contatos que você foi vítima de clonagem de perfil de *WhatsApp,* para que estes não repassem nenhum valor financeiro;

4. Golpe do perfil falso no Whatsapp

Neste golpe os criminosos não clonam o whatsapp da vítima, mas passam-se por ela criando um perfil falso, **utilizando fotos ou imagens**, usualmente, retiradas do próprio perfil de whatsapp da vítima ou de outras redes sociais.

Com a conta falsa os golpistas solicitam dinheiro à amigos e familiares observados nas redes sociais da vítima.

Orientações:

- Redefina a visualização da imagem da conta do Whatsapp apenas para contatos autorizados;
- Preferencialmente mantenha seus perfis nas redes sociais como privado;
- Desconfie de mensagens solicitando depósitos e transferências bancárias, principalmente para contas em nome de terceiros;

Fique atento a contas com fotos de conhecidos, mas com números diferentes;

O que fazer se cair neste golpe?

- Registre um boletim de ocorrência junto a Polícia Civil, mencionando o número do telefone do perfil fake;
- Alerte também, o mais rápido possível, os seus contatos sobre a existência de um perfil falso de *WhatsApp,* para que estes não repassem nenhum valor financeiro;

5. Golpe do "Phishing"

Criminosos costumam enviar mensagens (e-mails, SMS, Whatsapp) se passando por empresas privadas, bancos e agências governamentais. Nessas mensagens, é solicitado ao usuário que execute arquivos para efetuar atualizações ou que confirme informações de sua conta.

Ao clicar no endereço, a pessoa acaba sendo redirecionada para uma página falsa que irá: roubar as informações inseridas ou instalar um vírus no seu dispositivo.

Orientações:

- Nunca abra mensagens não solicitadas;
- Nunca clicar em nenhum dos links contidos no e-mail;
- Nunca fazer download ou executar qualquer arquivo anexado;

- Nunca responder ao e-mail;
- Nunca forneça suas informações pessoais;
- Mantenha o seu navegador, antivírus e sistema operacional sempre atualizados;
- Sempre confira se o endereço acessado é realmente o endereço correto.
- Implemente uma solução anti-spam para impedir que e-mails de phishing cheguem a rede;
- Nos casos de receber por e-mail institucional, encaminhar o e-mail suspeito para "cmti_rede@mpma.mp.br" para análise e bloqueio da origem.

O que fazer se cair neste golpe?

- Registre um boletim de ocorrência junto a Polícia Civil, fornecendo todas as informações possíveis.
- Procurar assistência especializada para verificação da presença de aplicativos maliciosos no seu aparelho;

6. Golpe utilizado para invadir WhatsApp Web

O aplicativo WhatsApp também pode ser utilizado em outros aparelhos pela opção WhatsApp Web. Para que isso seja possível, o usuário tem que utilizar o seu aparelho celular para ler um código QR gerado pela página oficial do aplicativo.

Criminosos clonam a página oficial do aplicativo e expõe um código QR falso que faz com que possam monitorar ou clonar o WhatsApp da vítima. Isso acontece com frequência em redes compartilhadas.

Orientações:

Como confirmar se esse monitoramento está ativo?

- Dentro do aplicativo, selecione os três pontos no canto superior direito e a opção WhatsApp Web;
- Caso apareça a mensagem última sessão ativa ou ativo agora, significa que alguém ativou o acesso web no seu telefone;
- Para desativar, basta selecionar a opção 'sair de todas as sessões;

Importante:

- Não utilize o seu aparelho para ler códigos enviados por estranhos!

7. Golpe da falsa ligação do banco

O criminoso liga para a vítima passando-se por funcionário do banco em que esta possui conta bancária. O criminoso informa que houve um problema sendo necessário a liberação de algumas chaves de acesso, e para tanto repassa o endereço de um site.

O site é falso e redireciona a vítima para uma página muito similar a página oficial do banco. Nesta página, todas as informações inseridas pela vítima são visualizadas pelo golpista (senhas, números de contas, cartões e etc.).

De posse dessas informações o golpista pode realizar pagamentos, transferências e compras on-line.

Orientações:

- Nunca forneça dados pessoais em ligações recebidas por telefone, caso necessite resolver algo relacionado à sua conta entre em contato pelos canais oficias de atendimento ou vá pessoalmente a uma agência bancária;

O que fazer se cair neste golpe?

- O mais rápido possível informe ao seu banco o ocorrido, e procure assistência especializada para verificação da presença de aplicativos maliciosos no seu aparelho ou computador;
- Registre um boletim de ocorrência junto a Polícia Civil, mencionando o número do telefone utilizado pelo golpista.

8. Golpe do Falso Sequestro

Os criminosos ligam para uma vítima e informam que sequestraram um familiar. Na mesma linha aparece outro criminoso com voz de choro passando-se pelo familiar sequestrado. Diante disto, a vítima nervosa e imaginando estar

falando com algum familiar acaba fornecendo informações (nome e grau de parentesco) que posteriormente são utilizadas pelos criminosos para dar maior autenticidade à farsa.

Como resgate do suposto sequestro os criminosos solicitam transferências em dinheiro e/ou que seja colocado créditos em alguns números telefônicos.

Neste tipo de golpe os criminosos solicitam que a vítima não desligue o celular, não entre em contato com a polícia ou outra pessoa. Em alguns casos até pedem que a vítima saia de casa e se desloque até outro local, ficando incomunicável.

Orientações:

- Ao receber ligações com esse padrão não forneça informações e desligue, logo em seguida tente entrar em contato com a pessoa supostamente sequestrada. Sempre solicite ajuda de outras pessoas, pois o nervosismo pode levá-lo a um erro;
- Caso não consiga contato pelo telefone, ligue para pessoas próximas do familiar supostamente sequestrado, pois eles podem saber onde ele está. Ainda que não consiga contato continue procurando em locais conhecidos (casa, trabalho, estabelecimentos próximos da residência e etc.).

O que fazer se cair neste golpe?

- Registre um boletim de ocorrência junto a Polícia Civil, fornecendo os números de telefone utilizados pelos golpistas e/ou contas informadas para transferências;

9. Extorsão por e-mail

Neste golpe, as vítimas são destinatárias de um e-mail onde consta que suas informações pessoais e/ou fotos íntimas foram acessadas por meio de ciber-ataques e serão liberadas para seus contatos, familiares e amigos nas mídias sociais, caso um resgate não seja pago.

A vítima neste mesmo e-mail é instruída a pagar o resgate em alguma forma de moeda de difícil rastreamento (a exemplo do *bitcoin*), em um curto espaço de tempo.

Orientações:

- Use soluções antivírus e habilite varreduras regulares de sistema e de rede;
- Mantenha os sistemas do seu computador e demais aparelhos atualizados;
- Nunca abra anexos nem clique em links em e-mails de spam ou em sites desconhecidos;
- Utilize senhas fortes.

Nos casos de receber por e-mail institucional, encaminhar o e-mail suspeito para "cmti_rede@mpma.mp.br" para análise e bloqueio da origem.

O que fazer se cair neste golpe?

- Registre um boletim de ocorrência junto a Polícia Civil, fornecendo todas as informações possíveis.

- Procurar assistência especializada para verificação da presença de aplicativos maliciosos no seu aparelho;

10. Orientações ao baixar aplicativos e receber boletos

Não instale aplicativos de origem desconhecida, pois o ideal é acessar a loja de aplicativos do seu celular (Google Play ou Apple store) e baixar por esse caminho. Muitos criminosos criam links e aplicativos falsos, parecidos com os reais, para aplicar golpes.

Ao receber boletos por meio de mensagens e e-mails fique atento:

- Se o endereço que aparece após o @ é o site oficial da empresa. **Ex.** financeiro@NomeDaLoja.com.br.
- Se o **código de barras** começa pelo **número do seu banco** (cada banco tem um número próprio).
- Se os valores estão muito diferentes (acima ou abaixo) daqueles que costuma pagar por um serviço ou uma mensalidade. Na dúvida, ligue para o serviço de atendimento da empresa ou instituição.
- Para sites com preços muito abaixo do mercado, pois estes merecem atenção dobrada!

11. Atenção para Compras através de Redes Sociais

Não é recomendável que os consumidores finalizem as compras pelas redes sociais, mas sim por meio de um **site seguro** e confiável;

Antes de comprar por aplicativo de troca de mensagens instantâneas como o WhatsApp, confirme por canais oficiais se o número pertence à empresa.

Orientações:

- **Pesquise antes! Verifique a Reputação da Empresa**
- Ao comprar em sites desconhecidos, é importante pesquisar o que outros consumidores relataram sobre a empresa nas redes sociais. Conhecer a opinião dos outros é uma forma de consultar a reputação do vendedor.
- Jamais insira dados pessoais - como nome, CPF, endereço e número de cartões - em página de pagamento de uma empresa desconhecida;
- Não forneça os dados pessoais para **qualquer e-mail** que chegue na caixa de entrada
- **Guarde os comprovantes das compras;** ao efetuar compras on-line, é importante capturar todas as telas (“**prints**”), e salvar o registro de todo o passo-a-passo até a finalização da compra;

- Guarde **todos os e-mails** de confirmação do pedido, pagamento e qualquer outra comunicação que receba da loja;
- **Use dispositivos seguros!** Evite usar wi-fi público e computadores de terceiros para efetuar compras. Só realize as transações em smartphones e computadores seguros.
- **Prefira utilizar Cartão Virtual!** Se for utilizar o cartão de crédito, dê preferência para o uso do cartão virtual. A numeração temporária ou diferente do cartão físico e do código de segurança gerados pelos aplicativos dos bancos são válidos exclusivamente para uso on-line.

12. Recebimento de chamada telefônica com o próprio número do celular

Neste tipo de golpe, o criminoso efetua ligação telefônica para a vítima, que por sua vez, verifica que o número de origem coincide com o seu. Nessa situação é extremamente importante que não se atenda esta ligação, pois caso isso ocorra, o estelionatário conseguirá, por meio de um *malware (*software malicioso*),* ter acesso aos dados pessoas da vítima.

Orientações:

- Recusar qualquer ligação originada de seu próprio número.
- Avisar aos seus contatos.

13. Golpe do sequestro de dados

O golpista se utiliza de um r*ansomware* (*malware*) que realiza a criptografia dos dados de computadores pessoais da vítima. Depois de criptografados, esses dados só poderão ser acessados por meio de uma chave de segurança, que fica em posse dos hackers.

Logo, para receber essa chave de acesso, o golpista cobra da vítima um resgate em criptomoedas. O problema é que mesmo realizando esse pagamento, não garantia para vítima ter de volta o acesso aos seus dados.

Orientações:

- **Não acessar sites suspeitos.**
- **Manter um backup atualizado dos arquivos do computador em um HD externo, pen drive ou outro dispositivo de armazenamento.**
- Não clicar em links duvidosos ou acessar e-mails de procedência desconhecida.

14. Falso cadastramento de Chave Pix

Por meio de links falsos encaminhados por aplicativos de mensagens, e-mail ou redes sociais, o golpista se faz passar por instituições bancárias, solicitando à vítima a realização de um suposto cadastro de sua chave PIX. Esses links, quando acessados, fornecem aos golpistas,

informações de senhas bancárias ou números de cartões de crédito, entre outras informações confidenciais das vítimas.

Orientações:

- **Não acessar sites, links duvidosos ou e-mails suspeitos.**
- Cadastrar a chave do PIX diretamente nos canais oficiais dos bancos ou *fintechs*, seja via aplicativo, internet banking, nas agências ou por contato com a central de atendimento, feito pelo próprio usuário.
- Em caso de dúvida, procurar o gerente ou a instituição.

15. Senha do Cartão de Crédito

Os dados da vítima são obtidos através de câmeras que filmam a senha quando estas são digitadas em lojas e caixas eletrônicos ou através de vírus, enviados por e-mail pelos golpistas. Com essas informações, o criminoso efetua e realiza compras em nome do real titular do cartão.

Outra maneira de golpe também ocorre quando o cartão de crédito novo é furtado durante seu processo de entrega. Nesse caso, o criminoso liga para a vítima se passando por funcionário da instituição bancária referente à bandeira do cartão, informando que aconteceram problemas na entrega e assim, solicita a senha do cartão para resolver o suposto problema, realizando transações em nome da pessoa.

Orientações:

- **Caso ocorra, comunicar imediatamente o fato à central de atendimento da operadora, pedir o bloqueio e anotar o número do protocolo, além de gerar um boletim de ocorrência.**
- Em compras pela internet, verificar se o site tem os selos de ambiente seguro.
- Verificar suas transações por meio de aplicativos para smartphones e acesso à internet banking diária ou semanalmente.
- Em lojas físicas, não deixar que o vendedor ou atendente levem seu cartão para algum lugar sem a sua supervisão. É comum os estelionatários aproveitarem a oportunidade para fotografar o cartão para realizar compras indevidas com seus dados na internet, já que esse tipo de ação online não exige sua senha. Além disso, é importante guardar com cuidado seu cartão para não correr o risco de perdê-lo e nunca emprestar o cartão de crédito para terceiros.
- Não enviar dados pessoais, senhas e acessos por ligação telefônica ou aplicativos de mensagens.
- Não preencher formulários na internet com dados pessoais sem verificar a origem.
- Informar à instituição bancária nos casos de demora acima do prazo estabelecido para a entrega do cartão.

- Não permitir que seus dados fiquem gravados dentro do sistema do site. É possível desativar o preenchimento automático de formulários dentro do seu próprio navegador ou no momento da compra.

Se você foi vítima entre em contato

Polícia Civil do Estado do Maranhão:

Departamento de Combate ao Crime Tecnológico: telefone (98) 3214-8657. Endereço: Rua do Correio, s/n, bairro de Fátima, São Luís – MA.

Delegacia de Defraudações: telefone: (98) 3214-8661 / 3214-8660. Endereço: Rua do Norte, nº 756, Centro, São Luís – MA.

Registre a Ocorrência: É importante fazer um *print* de tela que comprove o delito alegado, bem como o *print* da página do perfil do usuário que realizou a postagem falsa. Fique atento para que apareça a URL, que é o endereço da página.

Em casos envolvendo compras ou pagamento de boletos falsos, as vítimas podem tentar cancelar as transações com as próprias instituições bancárias e realizar denúncia formal da prática junto a Polícia Civil, bem como no **PROCON/MA**, através do site: www.procon.ma.gov.br ou aplicativo PROCON MA.

TELEFONE ÚTEIS

CIOPS (PM): **190**
BOMBEIROS: **193**
SAMU: **192**
PRF: **191**
SMTT (GTT): (98) **98607-9807**

Corrdenadoria de Assuntos Estratégicos
e Inteligência (CAEI): **3219-1797**

Segurança Institucional/PGJ: **3219-1796**
Vídeo Monitoramento/PGJ: **3231-4188**

REFERÊNCIAS:

COMITÊ GESTOR DA INTERNET NO BRASIL. **Cartilha de Segurança para Internet**. São Paulo.2012.

GOVERNO DO ESTADO DO RIO DE JANEIRO: **Cartilha Contra Crimes Virtuais**. Rio de Janeiro-RJ. 2020.

MINISTÉRIO PÚBLICO DO ESTADO DO PERNAMBUCO. **Cartilha de Proteção contra golpes virtuais e presenciais.** Recife-PE. 2021

POLÍCIA CIVIL DE SANTA CATARINA: **Proteja-se de Golpes: a Informação é a melhor forma de se proteger**. Santa Catarina-SC.2021

MPMA Ministério Público do Estado do Maranhão

CAEI
COORDENADORIA DE ASSUNTOS ESTRATÉGICOS E INTELIGÊNCIA