MP PE
Ministério Público de Pernambuco
CONECTADO COM A INCLUSÃO

CARTILHA

PREVENÇÃO A GOLPES VIRTUAIS E PRESENCIAIS

Atitudes para segurança pessoal e de dados

1ª edição

MINISTÉRIO PÚBLICO DE PERNAMBUCO

Rua do Imperador D. Pedro II, 473, Edf. Promotor de Justiça Roberto Lyra,
Santo Antônio, Recife, PE – CEP: 50010-240, Tel (81) 3182.7000 - www.mppe.mp.br

CARTILHA

PREVENÇÃO A GOLPES VIRTUAIS E PRESENCIAIS

Atitudes para segurança pessoal e de dados

1ª edição

Recife, 2021

MP PE
Ministério Público de Pernambuco
CONECTADO COM A INCLUSÃO

Redação e organização

Major PM Sérgio Souza dos Santos – Gerente Ministerial de Áreas e Instalações

Revisão Técnica

Coronel PM André Luiz Freitas Ferreira – Assistente Militar e Policial Civil

Créditos

Revisão ortográfica | Andréa Corradini

Projeto gráfico/ diagramação | Leonardo MR Dourado

Ilustração capa | Upklyak/ Freepik

Ilustrações internas | Freepik

FICHA CATALOGRÁFICA

P452c PERNAMBUCO. Ministério Público. Assistência Militar e Polícia Civil.

Cartilha prevenção a golpes virtuais e presenciais: atitudes para segurança pessoal e de dados. / Redação e texto Sérgio Souza dos Santos ; Revisão técnica, André Luiz Freitas Ferreira ; [recurso eletrônico]. – Recife: Procuradoria-Geral de Justiça, 2021.

66 p. ; il.

1. Golpe Virtual - Prevenção. 2. Golpe Presencial - Prevenção. 3. Crime de Informática. 4. Clonagem WhatsApp. 5. Segurança de dados. 6. Ministério Público. Procuradoria-Geral de Justiça. 7. Assistência Militar e Polícia Civil – AMPC. I. Título. II. SANTOS, Sérgio Souza dos.

MPPE-BIB CDDIR 001.6

Bibliotecárias: Rosa Dalva Rivera de Azevedo CRB-4/931 e
Analuci da Conceição Goes CRB-4/2286

Sumário

Introdução

A tecnologia traz inúmeras vantagens de conexão, ganho de tempo e facilidade na execução de tarefas cotidianas. Em paralelo, seu uso também traz inúmeros riscos. Muitas pessoas têm sido vítimas dos mais variados golpes em ambientes virtuais: clonagem de aplicativos, extorsões e sequestros de dados são alguns exemplos cada vez mais comuns.

Dentro desse contexto, a Assistência Militar e Policial Civil (AMPC) do Ministério Público de Pernambuco elaborou a presente cartilha, com dicas de segurança contra golpes virtuais e presenciais. O material tem o objetivo de promover uma cultura de segurança institucional e prevenir os integrantes do Ministério Público de Pernambuco, seus familiares e também a população contra fraudes. Fique atento às dicas, adote as ações preventivas indicadas. Desejamos que seja um instrumento importante para a criação de uma atitude de atenção e segurança.

Principais golpes

Clonagem do WhatsApp

Através de uma ligação telefônica ou mensagem de texto, o falsário se passa por representante de um site promocional, site de compras ou acaba enviando falsos convites para eventos badalados. Assim, convence o usuário a informar, via WhatsApp, os seis números que lhe foram enviados por SMS. Após obter essa informação, o golpista consegue clonar o aplicativo de mensagens WhatsApp.

A segunda fase do golpe consiste no envio de mensagens oriundas do WhatsApp clonado, onde o criminoso se passa pelo real titular da conta, solicitando a seus contatos ajudas financeiras em caráter de urgência, que em muitos casos são atendidas.

Dicas de prevenção

- Não compartilhar qualquer código ou senha com desconhecidos, sobretudo, via aplicativos de mensagens.
- Ativar a função "Verificação em duas etapas" no WhatsApp:
- No menu de três pontos clique em "Configurações"; busque "Conta" e então escolha "Verificação/ Confirmação em duas etapas".
- Pressione "Ativar" e crie uma senha de seis dígitos para a conta do WhatsApp.

- Confirme e em seguida disponibilize um endereço de email válido para o caso de esquecer o código.
- Clique em "Avançar" e confirme seu endereço de e-mail, em "Salvar".
- Não compartilhar informações pessoais através de aplicativos de mensagens.
- Alertar imediatamente os contatos sobre a clonagem do aplicativo WhatsApp, caso ocorra, a fim de evitar o golpe.
- No caso de ser surpreendido com pedido de ajuda financeira de algum contato do WhatsApp, efetuar ligação telefônica para confirmar a real necessidade e nunca proceder a eventual transferência de recursos sem ter a devida comprovação.

Foto do perfil do WhatsApp

O criminoso usa a foto do perfil do aplicativo de mensagem da vítima em outra conta. Em seguida, informa aos parentes e amigos que mudou de número. Com isso, o estelionatário se passa pela pessoa que teve a foto furtada, solicitando a familiares e conhecidos quantias em dinheiro, alegando urgência.

Dicas de prevenção

- Mudar a configuração do WhatsApp para que a foto do perfil só apareça para os contatos salvos em sua agenda.
- Desconfiar da aproximação repentina de pessoas na internet, principalmente se elas pedirem ajuda financeira ou acesso a seus dados pessoais.
- Evitar enviar dados pessoais por aplicativo de mensagem ou ligação telefônica.
- Alertar imediatamente os contatos sobre o uso indevido do perfil no aplicativo WhatsApp, caso ocorra, a fim de evitar o golpe.
- Não acessar links ou emails suspeitos.

Ligação do próprio celular

O criminoso efetua ligação telefônica para a vítima, que por sua vez, percebe que o número de origem coincide com o seu. Não se deve atender ligação originada do seu próprio número. Com apenas 10 segundos o estelionatário consegue acesso aos dados pessoais da vítima.

Dicas de prevenção

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

Pharming

O pharming acontece quando a vítima tem a sua navegação na internet redirecionada para sites falsos, que pode ter como consequência o vazamento de dados pessoais com possível perda financeira.

Dicas de prevenção

- Escolher um provedor de internet confiável.
- Verificar se há erros no endereço do site que se pretende acessar.
- Ao desconfiar de um site, inclusive de um banco, realizar login com uma senha errada. Como um site falso não tem como conferir a sua senha, a próxima tela mostrará que é golpe.

Phishing

O criminoso envia um link ou email com vírus que direcionam as vítimas a sites falsos, em geral solicitando a atualização de dados juntos a instituições financeiras ou administradoras de cartão de crédito.

Dicas de prevenção

- Desconfiar de mensagens com conteúdo financeiro.

- Não acessar sites, links duvidosos ou emails suspeitos.
- Procurar o banco ou administradora do cartão de crédito para confirmar qualquer contato via mensagem de texto ou ligação telefônica.
- Manter o antivírus e *firewall* atualizados.

Sequestro de dados (Ransoware)

O Ransomware é um software malicioso (*malware*) que criptografa os dados de computadores pessoais da vítima. Depois de criptografados, esses dados só poderão ser acessados através do fornecimento de uma chave de segurança, que fica em posse dos hackers. Para receber essa chave de acesso é necessário pagar um resgate em criptomoedas e acreditar que o malfeitor terá uma conduta ética. O problema é que após a encriptação dos dados tudo foge do controle. Por sua vez, a vítima não consegue ter acesso aos seus dados por estarem bloqueados.

Dicas de prevenção

- Manter um *backup* atualizado dos arquivos do computador em um HD externo, pen drive ou outro dispositivo de armazenamento.
- Não acessar sites suspeitos.
- Não clicar em links duvidosos ou acessar emails de procedência desconhecida.
- Manter os mecanismos de proteção ativados e atualizados (antivírus e *firewalls*)

Engenharia social

O criminoso observa a vítima em suas redes sociais, conhecendo seus hábitos. O que é muito comum hoje em dia, haja vista a naturalidade como se expõem as atividades cotidianas através das mais diversas plataformas, facilitando a ocorrência dos chamados crimes digitais. De posse de informações preciosas, o estelionatário comete a fraude.

Dicas de prevenção

- Não divulgar informações confidenciais ou mesmo informações aparentemente não confidenciais sobre você ou sua empresa, sobretudo em redes sociais.
- Não acessar sites, links duvidosos, propagandas ou emails suspeitos.

Aplicativos de relacionamento

O criminoso cria uma conta em um aplicativo de relacionamentos, aproximando-se da vítima fingindo interesse afetivo. Conquista sua confiança e após algum tempo apresenta uma história em que alega estar precisando de dinheiro urgente para resolver algum problema sério, muitas vezes relacionado à saúde de algum familiar. Conseguindo a quantia solicitada, o falsário desaparece, deixando o prejuízo financeiro. Em época de pandemia, a necessidade de isolamento por conta da Covid-19 tem sido uma desculpa bastante usada para que o estelionatário se afaste da vítima.

Dicas de prevenção

- Estar atento a promessas de amores instantâneos.
- Atentar para a possibilidade de fotos falsas de perfis.
- Manter sistemas e *firewall* atualizados.

Extorsão por nudes ou sextorsão

Em geral, o criminoso inicia uma conversa com a vítima, através de redes sociais, mudando sua identidade, utilizando perfil falso e quase sempre fotografias de pessoas com beleza exuberante. Com o tempo e após conquistar certa confiança, iniciam um jogo de troca de fotos sensuais. A partir de então, o criminoso passa a praticar a extorsão, ameaçando divulgar as fotos íntimas em redes sociais e grupos de Whatsapp, caso a vítima não deposite uma quantia em dinheiro.

Dicas de prevenção

- Evitar adicionar e conversar em redes sociais com perfis desconhecidos.
- Evitar conversar com prefixos telefônicos desconhecidos.
- Não trocar fotografias, que possam ter conotação íntima, através do WhatsApp ou Messenger.
- Jamais fazer depósitos, transferências ou pagamentos para desconhecidos.
- Não divulgar hábitos e rotinas em redes sociais.
- Não armazenar fotos e vídeos íntimos em seu celular, computador ou notebook. Esses materiais, quando recolhidos para manutenção ou roubados, podem permitir que outras pessoas tenham acesso a esses arquivos.

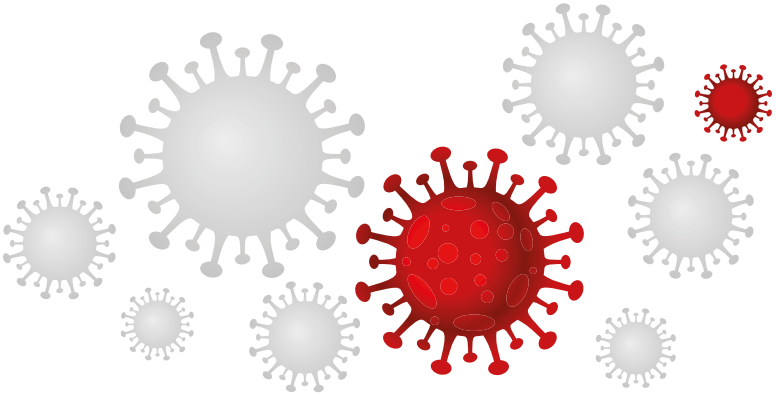
- Evitar participar de chamadas de vídeo com desconhecidos.
- Se for vítima de algum golpe, não apagar as conversas, procurar a polícia e registrar ocorrência.

Agendamento da vacina contra a Covid-19

O golpista liga para a vítima, passando-se por funcionário do Ministério ou Secretaria de Saúde, oferecendo o agendamento para a vacina contra a Covid-19. Eles solicitam dados pessoais e enviam por SMS um código ou um link de confirmação para o celular, pedindo para que a pessoa informe os números enviados ou clique no link, o que possibilita a clonagem do aplicativo de mensagens ou o acesso aos dados sigilosos do celular.

Dicas de prevenção

- Atentar que os órgãos de saúde pública não telefonam para marcar vacinação contra Covid-19 nem pedem confirmação de códigos enviados por SMS.
- Não fornecer dados pessoais através de ligação ou mensagem.
- Não acessar links duvidosos ou emails suspeitos.
- Ativar o mecanismo de verificação em duas etapas do aplicativo de mensagens.



Falsa pesquisa Covid-19

O golpista envia um email para a vítima alegando se tratar de um estudo para identificar a efetividade da vacina contra a Covid-19. O email traz ainda a informação de que o resultado do estudo auxiliaria no planejamento das próximas campanhas de vacinação, principalmente em situações de pandemia. Por fim, traz um link para a suposta pesquisa.

Dicas de prevenção

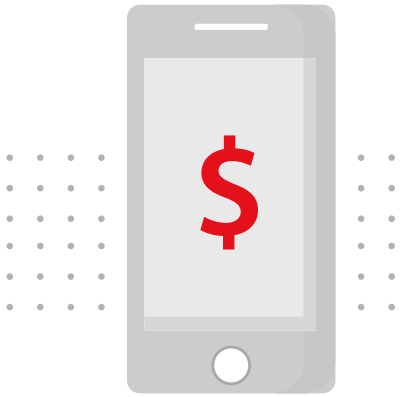
- Não acessar sites suspeitos disponíveis na internet.
- Não acessar links duvidosos ou emails suspeitos.
- Atentar que, em geral, os canais de comunicação dos órgãos públicos trazem o domínio *.org*, ao invés de *.com*.

Atualização do aplicativo *Caixa Tem*

A vítima recebe um SMS supostamente da Caixa Econômica Federal com um link para atualização do aplicativo *Caixa Tem*. O golpista pede para quem é beneficiário do auxílio emergencial acesse o link para conseguir atualizar o aplicativo, alegando que, se a pessoa não atualizar esse aplicativo, não receberá novas parcelas. Ao clicar no link, informações pessoais são obtidas pelos criminosos, efetivando o golpe.

Dicas de prevenção

- A Caixa Econômica Federal alerta que não envia nenhum tipo de SMS que tenha relação com o auxílio emergencial, apenas e-mails, e, mesmo assim, apenas se o beneficiário autorizar.
- Não fornecer dados pessoais através de ligação ou mensagem.
- Não acessar links duvidosos ou emails suspeitos.
- Ativar o mecanismo de verificação em duas etapas do aplicativo de mensagens.



Golpe do auxílio emergencial

Antes do primeiro acesso do beneficiário à sua conta poupança social digital, criada pela Caixa Econômica Federal, o golpista, de posse do CPF da vítima, cria um email e consegue desviar o dinheiro que seria depositado na conta do cidadão.

Dicas de prevenção

- Manter o cadastro de beneficiário atualizado, conforme instruções da Caixa Econômica Federal.
- A atualização deverá ser realizada inteiramente através do aplicativo *Caixa Tem*, sem a necessidade de comparecimento a qualquer agência.
- Não fornecer dados pessoais a estranhos.

Cadastro da chave do PIX

O criminoso envia links falsos por meio de aplicativos de mensagens, email ou redes sociais, fazendo se passar por instituições bancárias, solicitando à vítima a realização de um suposto cadastro de sua chave PIX. O golpe prossegue quando os links levam a sites falsos de bancos ou à instalação de aplicativos maliciosos, que roubam dados pessoais e financeiros. O objetivo é pegar senhas bancárias ou números de cartões de crédito, entre outras informações confidenciais.

Dicas de prevenção

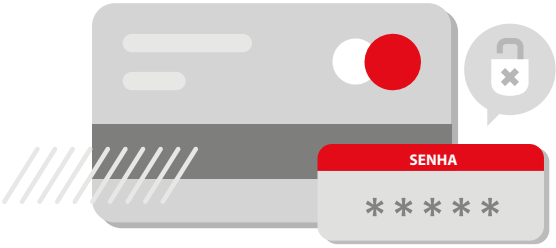
- Não acessar sites, links duvidosos ou emails suspeitos.
- Cadastrar a chave do PIX diretamente nos canais oficiais dos bancos ou fintechs, seja via aplicativo, internet banking, nas agências ou por contato com a central de atendimento, feito pelo próprio usuário.
- Em caso de dúvida, procurar o gerente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

Dinheiro em dobro após transferência por PIX

Mensagens de texto, imagens e vídeos são disseminadas por hackers com a alegação de que falhas nos sistemas de instituições financeiras brasileiras e do próprio Pix poderiam levar a uma devolução em dobro de valores transferidos, bastando apenas enviar montantes para contas específicas. No entanto, as chaves do Pix em questão pertencem aos próprios falsários e a devolução, obviamente, não acontece.

Dicas de prevenção

- Manter a desconfiança e ignorar mensagens desse tipo.
- Nunca transferir quantias para pessoas desconhecidas.



Cartão de crédito

O criminoso obtém os dados da vítima através de câmeras que filmam a senha sendo digitada em lojas e caixas eletrônicos ou através de vírus, enviados por email para obter dados pessoais. Com essas informações, o falsário realiza compras e efetua saques em nome do real titular do cartão. Outra modalidade de golpe ocorre quando o cartão 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.

Dicas de prevenção

- 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.

- 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.
- Verificar suas transações por meio de aplicativos para smartphones e acesso à internet banking diária ou semanalmente.
- Não acessar sites, links duvidosos ou emails suspeitos.
- 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.

Boletos falsos

O criminoso consegue a informação de que a vítima paga determinada dívida através de boleto bancário e emite um falso com dados que não correspondem aos do real destinatário, mas de um falsário.

Dicas de prevenção

- Sempre emitir os boletos no site oficial da empresa ou do banco que está fazendo a cobrança.
- Não acessar sites de recálculo de boleto atrasado, em geral são falsos.
- Não acessar links duvidosos ou emails suspeitos.
- Antes de efetuar o pagamento, verificar se os três primeiros números da sequência correspondem ao código do banco que emitiu o boleto.
- Conferir se os dados do beneficiário ou da pessoa que vai receber o dinheiro estão corretos.
- Verificar se o código de barras que fica na região superior do documento é idêntico ao que aparece na parte inferior.

Chip roubado

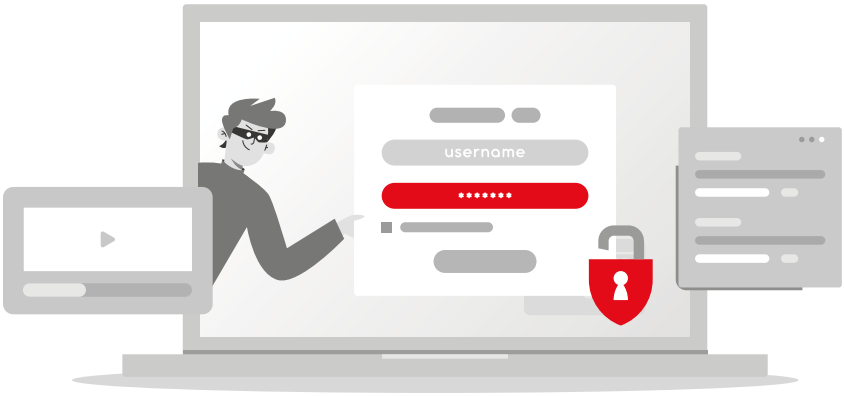
O criminoso adquire um chip novo e liga para a operadora se passando pelo dono do chip original. Em seguida, alega que teve o celular extraviado. Assim, a central reativa o antigo número no novo chip. Com isso, o golpista tem acesso aos grupos e à lista de contatos da pessoa no WhatsApp.

Quando o novo chip é ativado, o original é bloqueado. Essa ação se dá sem a necessidade de invadir qualquer dispositivo e correndo pouco risco.

De posse do número original, o criminoso entra em contato com amigos e familiares da vítima para extorqui-los. Na maioria das vezes, o estelionatário diz que está precisando de dinheiro com urgência. É importante frisar que o golpista acaba utilizando a foto e o número de telefone do familiar ou amigo do alvo da extorsão. Há casos, inclusive, em que o criminoso ainda extorque o próprio dono do chip para devolver o número.

Dicas de prevenção

- Ativar a verificação em duas etapas no aplicativo WhatsApp.
- Evitar repassar informações pessoais por aplicativos de mensagem ou ligação telefônica a desconhecidos.



Sites fraudulentos

O estelionatário envia links por email ou por aplicativos de mensagens e que são páginas praticamente idênticas às de grandes lojas online. O consumidor irá comprar, mas nunca receberá o produto e pior: não terá para quem processar ou como resgatar o valor pago.

Dicas de prevenção

- Não acessar sites, links duvidosos ou emails suspeitos.
- Ter cuidado com propagandas recebidas que possam se caracterizar como spam.
- Manter antivírus e *firewall* atualizados.

Sites de leilão e vendas de produtos

O estelionatário cria uma página que simula uma plataforma de leilões on-line, bem como utiliza ferramentas de pagamento, já que os sites falsos costumam exibir formas de pagamento no rodapé da página, como ícones de boleto e cartão de crédito. Assim, cria um site falso, com telefone e e-mail para tentar passar credibilidade. Adota também um nome falso de empresa e, em certos casos, utiliza até nomes de empresas já existentes e reconhecidas no mercado. Os golpes incluem mercadoria comprada e não entregue, produto ou serviço diferente da venda e clonagem de cartão.

Dicas de prevenção

- Ter atenção ao digitar o site de compras e certificar-se que a plataforma a ser utilizada realmente é segura.
- Conferir o link do site suspeito em portais de busca e verificação de fraudes. Os projetos "Fraude em Leilões" e "Leilão Seguro", por exemplo, mantêm uma lista com sites de leilões falsos.
- Entrar em contato com o leiloeiro responsável pelo evento.
- Verificar o cadastro do leiloeiro oficial da empresa junto à JUCEPE em Pernambuco.
- Conferir o edital do leilão.

- Não divulgar sua chave de segurança de acesso ao site de leilão a terceiro.
- Buscar toda a comprovação necessária do bem a ser adquirido antes de pagar.
- Analisar a própria empresa leiloeira para ver sua reputação no mercado.

Vale-presentes

O criminoso envia um link oferecendo vales-presentes falsos, em geral de grandes redes de supermercados ou de lojas conhecidas. Ao clicar no link e passar suas informações pessoais a vítima cai no golpe.

Dicas de prevenção

- Desconfiar de promoções oferecidas através de mensagens.
- Não acessar sites, links duvidosos ou emails suspeitos.
- Antes de clicar em qualquer link, procurar saber em fontes oficiais, se a promoção realmente existe.
- Manter antivírus e *firewall* atualizados.

Defeito na linha telefônica

O falsário liga para o telefone fixo da vítima informando que sua linha encontra-se com problema. Em seguida, passa um código para que a pessoa digite. Essa ação provoca a transferência da chamada para o telefone do criminoso através da ferramenta "siga-me". Com isso, o golpista passa a utilizar a linha da vítima para falsos sequestros, extorsões, etc.

Dicas de prevenção

- Atentar para o fato de que as operadoras telefônicas não ligam para os usuários relatando problemas na linha.
- Não digitar qualquer sequência de números informada por pessoas desconhecidas.

Bilhete premiado

Consiste na troca de uma quantia em dinheiro da vítima por um bilhete supostamente premiado. O criminoso afirma para a vítima que está de posse de um bilhete de loteria premiado, mas precisa viajar imediatamente e isso lhe impede de resgatar o suposto prêmio, convencendo a vítima a comprar-lhe o falso bilhete.

Dicas de prevenção

- Desconfie de dinheiro, benefício ou recompensa oferecidos por estranhos na porta de bancos e casas lotéricas.
- Diante de qualquer atitude suspeita, comunique à Polícia.

Assaltos a entregadores

Entregadores são rendidos por assaltantes e têm suas motocicletas roubadas, durante o trajeto ou mesmo no endereço da entrega. Os assaltantes tomam o lugar do verdadeiro entregador a fim de assaltar também o destinatário da encomenda.

Dicas de prevenção

- Ao solicitar alguma encomenda, pedir o nome do entregador e confirmá-lo, via interfone (se existir) quando de sua chegada.
- Não abrir o portão a pedido de um estranho com destino a apartamento vizinho, alegando que o interfone está com problemas.

Carro quebrado

O golpista faz uma ligação telefônica para um número aleatório. Ao ser atendido, diz que é um parente da pessoa que atendeu o telefone. Durante a breve conversa, alega que seu veículo apresentou problemas no meio de uma estrada e que na ocasião não dispõe de dinheiro para acionar um guincho ou mecânico. Essa informação faz com que a pessoa deposite certa quantia na conta do criminoso.

Dicas de prevenção

Não efetuar qualquer depósito ou transferência bancária sem ter a certeza da identidade do destinatário.

Evitar tratar de assuntos de cunho financeiro por telefone ou aplicativos de mensagens.

Colisão de trânsito

O criminoso dirige atrás do veículo da vítima e encosta na traseira do automóvel, provocando uma pequena colisão, em local oportuno para a ação do roubo. A vítima é assaltada quando desce do carro.

Dicas de prevenção

- Dependendo da situação e lugar, é melhor não descer e ficar no prejuízo, pois os danos serão menores e a vítima não coloca sua vida em risco.
- Quando em viagem, se a colisão não interferir no funcionamento do veículo, parar somente em locais seguros, tais como postos policiais, postos de gasolina ou locais habitados.
- Se possível, informar para um parente ou pessoa de confiança o trajeto que está percorrendo durante a viagem.

Documentos pessoais

Aproveitando descuidos para furtar documentos pessoais ou mesmo copiando os dados no momento de algum cadastro, os criminosos se utilizam dos dados para auferirem vantagens indevidas através de empréstimos bancários sem a intenção de pagar, cartões de créditos, crediários, etc.

Dicas de prevenção

- Não deixar documento com desconhecido quando você não estiver por perto.
- Não disponibilizar dados pessoais para pessoas estranhas.
- Não fornecer ou confirmar informações pessoais por telefone.
- Nunca perder de vista seus documentos de identificação quando solicitados para protocolos de ingresso em determinados ambientes, cadastros ou para quaisquer negócios.
- Entregar fotocópias em preto e branco.
- Entregar cópias com duas linhas paralelas sobre os documentos.

Empréstimo consignado

O criminoso deposita indevidamente uma quantia na conta da vítima, graças a algum cadastro realizado anteriormente em alguma instituição financeira ou correspondente bancário, o que, em muitos casos, possibilita o acesso à senha e login. Nos meses subsequentes são realizados descontos na conta ou no cartão de crédito da vítima referentes ao empréstimo irregular.

Dicas de prevenção

- Procurar sua instituição bancária no caso de qualquer quantia de origem duvidosa depositada em sua conta.
- Não permitir que pessoas estranhas preencham seus cadastros, ou tenham acesso a suas senhas e logins.

Envelope vazio

O golpista efetua a compra de determinado objeto ou serviço, realiza o depósito equivalente em um envelope sem o dinheiro, em seguida apresenta o comprovante de pagamento e a vítima entrega o bem ou presta o serviço, e só depois descobre que tudo não passou de um golpe.

Dicas de prevenção

- Entregar a mercadoria ou prestar o serviço apenas quando o valor acertado estiver liberado e disponível em sua conta.
- Em caso de dúvidas, entrar em contato com o gerente do seu banco.

Falsa multa de trânsito

O golpista tira fotos de placas de veículos e, com a ajuda de despachantes, descobre os endereços dos proprietários. Com isso, enviam multas falsas para os motoristas pagarem, cujo valor vai, na realidade, para a conta do falsário ou de um coautor.

Dicas de prevenção

- Consultar o site oficial do DETRAN para verificar, por meio do número da placa e Renavam (Registro Nacional de Veículo Automotor), se há de fato algum registro de infração de trânsito.
- Caso o boleto indique outro órgão, como as prefeituras, é importante fazer pesquisas também nos sites do Departamento de Estradas e Rodagem (DER) e da Polícia Rodoviária Federal (PRF).
- Ficar atento, pois sempre que uma infração é registrada, primeiro é enviada ao proprietário uma notificação de autuação, com campo para indicação de condutor. Somente após o prazo para a indicação será encaminhada a notificação de penalidade, que é o boleto para pagamento da infração de trânsito cometida.

Falso empréstimo

Os criminosos entram em contato diretamente por telefone, oferecendo condições especiais de empréstimo. Ao longo da conversa, o criminoso já possui valores fechados para cada parcela e solicita o pagamento de taxas antecipadas para liberação do valor em conta. Ao concordar com o empréstimo e realizar o pagamento, o consumidor é enganado e não consegue reaver o seu dinheiro.

O pagamento de valores antecipados é, sem sombra de dúvida, o principal golpe do empréstimo. Aqui, os golpistas informam ao consumidor que para ter o seu empréstimo aprovado, ele precisa pagar antecipadamente o valor referente ao IOF (Imposto sobre Operações Financeiras) do contrato. Por saber que realmente há essa cobrança, o consumidor antecipa o pagamento, mas não recebe nenhum valor como empréstimo.

Dicas de prevenção

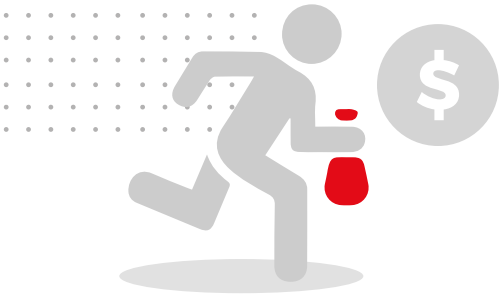
- Atentar que empresas certificadas pelo Banco Central não cobram taxas antecipadas para liberação de crédito, tampouco depósitos de valores em conta corrente de pessoas físicas.
- Nunca depositar quaisquer quantias em contas desconhecidas.
- Desconfiar se estiver negativado e as condições ofertadas para empréstimo forem muito atraentes.

Falso funcionário de banco

Em filas de caixas eletrônicos, sobretudo as destinadas a depósitos bancários, o criminoso se passa por funcionário do banco e até organiza a fila de clientes. Em seguida, recolhe as guias de depósitos com o dinheiro, pedindo que o cliente aguarde o recibo, porém o falsário sai rapidamente do local levando as quantias que lhe foram entregues.

Dicas de prevenção

- Manter sigilo sobre a senha da conta bancária.
- Não aceitar a ajuda de estranhos em agências bancárias.
- Se for necessário aceitar a ajuda, certificar-se de que se trata de fato de funcionário do banco.



Falso sequestro

O criminoso liga para a vítima, que, ao atender, escuta ameaças do criminoso e ao fundo gritos e choro da suposta pessoa sequestrada. A vítima, em desespero, acaba falando o nome do ente querido supostamente sequestrado e isso favorece o golpe. Em geral, são cometidos por reclusos do sistema prisional.

Dicas de prevenção

- Não confirmar dados nem falar nomes de familiares.
- Desligar o telefone e procurar a pessoa supostamente sequestrada.
- Nunca prolongue chamadas com desconhecidos e não forneça dados pessoais para cadastros.
- Antes de qualquer atitude, procurar ajuda de alguém que não esteja envolvido emocionalmente com a situação.

Familiar internado em hospital

O criminoso efetua ligação telefônica para a vítima se passando por funcionário ou médico do hospital onde um familiar encontra-se internado e solicita um depósito referente a um medicamento ou procedimento não coberto pelo plano de saúde.

Dicas de prevenção

- Não realizar depósitos antes de checar a veracidade das informações.
- Ficar atento ao receber ligações de números desconhecidos acerca de assuntos financeiros ou comerciais.
- Verificar a veracidade da informação junto ao hospital.
- Não repassar seus dados pessoais, principalmente número de contas bancárias e cartões de crédito.
- Atentar para o fato de que hospitais não fazem cobranças de procedimentos extras ou de medicações via telefone.
- Entrar em contato com o plano de saúde para verificar a veracidade da informação.

Parentes em dificuldade

O estelionatário se passa por um parente em apuros financeiros e pede, por telefone, que a vítima, em geral, pessoa de mais idade, deposite uma quantia em dinheiro para socorrê-lo.

Dicas de prevenção

- Não trate assuntos financeiros ao telefone.
- Desligar a ligação e em seguida, contactar a pessoa conhecida.
- Não depositar dinheiro na conta de desconhecidos

Ingresso em Escolas Militares

Em geral, a cilada se inicia dentro de escolas. Na ocasião, o criminoso cita os benefícios oferecidos pelas Forças Armadas, tais como assistência médica e odontológica, moradia, transporte, alimentação e ajuda de custo. Assim, convence os jovens a fazerem uma prova para ingresso no Exército, Marinha ou Aeronáutica, mediante o pagamento antecipado de uma quantia em dinheiro. Todavia, tudo não passa de um golpe.

Dicas de prevenção

- Atentar para o fato de que o ingresso nas Escolas Militares das Forças Armadas acontece por meio de concurso público.
- Buscar informações sobre o ingresso nas Forças Armadas através dos sites oficiais de suas instituições ou dos editais dos concursos.

Golpe do motoboy

O criminoso liga para a vítima se passando por atendente do banco, informando que seu cartão foi clonado. O suposto funcionário, então, a orienta a ligar no telefone fornecido como SAC do banco para cancelar a transação. Ao ligar no número informado, a vítima é atendida por outro suposto membro da instituição, que confirma todos os seus dados pessoais e últimas compras realizadas, pedindo para que ela entregue o suposto cartão clonado, cortado ao meio, para um motoboy que se deslocará até sua residência. Com as informações do cartão, compras são realizadas.

Dicas de prevenção

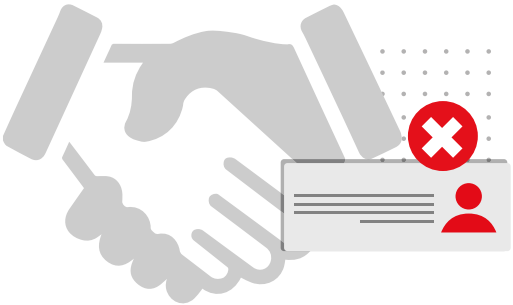
- Não fornecer dados pessoais através de ligação ou mensagem.
- Confirmar com o banco ou com a operadora do cartão o conteúdo das informações repassadas em ligações recebidas.
- Em geral, os bancos não solicitam a devolução de cartão clonado ou avariado. Normalmente os usuários são orientados a destruí-los.

Oferta de emprego

Um email é enviado à vítima, tratando de uma oferta de emprego, que geralmente não é da sua área de conhecimento, mas para uma vaga de comprador ou um cargo parecido. Depois de aceitar, a vítima recebe um pagamento em cheque ou ordem de pagamento com valor superior ao que o "empregador" ofereceu. Ele pede a devolução da diferença, e então a vítima descobre que o cheque ou a ordem de pagamento eram falsos, ficando sem o dinheiro que foi enviado ao falso empregador.

Dicas de prevenção

- Se aceitar um trabalho, nunca depositar cheques suspeitos antes de confirmar sua autenticidade.
- Verificar o saldo de sua conta para confirmar o suposto depósito.
- Sempre que pedirem a devolução de qualquer "diferença", será sinal de golpe.



Passagem aérea

O estelionatário oferece a passagem com um valor muito mais baixo do que o normal, às vezes alegando ser fruto de bônus de cartão de milhagem ou então utilizando o nome de uma empresa conhecida no mercado. A vítima é atraída pelo valor e acaba efetuando a falsa compra de uma passagem que nunca chega.

Dicas de prevenção

- Não acreditar em ofertas generosas, sobretudo vindas de pessoas desconhecidas.
- Somente comprar passagens diretamente de empresas aéreas ou agências de turismo comprovadamente idôneas.

Pecúlio ou ação judicial

O criminoso envia uma carta à vítima, normalmente com um timbre falso do Tribunal de Justiça Estadual ou escritório de advocacia, informando que ela tem um saldo a receber das carteiras de pecúlio ou ação judicial coletiva. Para receber a quantia informada, a vítima tem que fazer um depósito em conta indicada pelo estelionatário, com quantia referente às custas administrativas e processuais.

Dicas de prevenção

- Não fornecer dados pessoais. Assuntos de caráter financeiro devem ser tratados, de preferência, pessoalmente.
- Não realizar qualquer depósito sem ter a certeza da origem da solicitação.
- A prática judicial não prevê ligações telefônicas informando quanto ao êxito das ações.

Pirâmide financeira

A vítima é apresentada a um investimento com ganhos fáceis e extremamente tentadores. O golpe consiste no recrutamento de novos membros para o grupo. Um investidor indica um novo membro que ficará no nível abaixo dele, por sua vez, este integrante tem a meta de chamar mais pessoas para ocupar o degrau abaixo. Em determinado momento, a estrutura do grupo não se sustenta em razão da quantidade de pessoas e os que entram por último, em geral, acabam no prejuízo.

Dicas de prevenção

- Buscar formas confiáveis de investir dinheiro.
- Desconfiar de propostas financeiras com ganhos fáceis.
- Observar que a pirâmide financeira configura crime contra a economia popular.

Recebimento de ações da Petrobrás

O criminoso entra em contato com a vítima, identificando-se como funcionário da Petrobras e alegando que ela teria direito a receber ações da estatal, mas que para isso teria que realizar um depósito em conta corrente informada pelo golpista, a título de taxas e impostos.

Dicas de prevenção

- Atentar para o fato de que empresas, em geral, não ligam para informar acerca de recebimento de ações e se o fizerem, não solicitam qualquer quantia antecipada para pagamento de supostas taxas ou encargos.
- Não confiar em emails recebidos referentes a assuntos financeiros ou comerciais.
- Não acessar sites, links duvidosos ou emails suspeitos.

Troca de maquineta em estabelecimentos comerciais

Aproveitando-se de descuido do lojista, o criminoso, de posse de uma maquineta ativa e com as mesmas características da utilizada no estabelecimento comercial ou prestador de serviço, efetua a troca dos aparelhos e com isso, todos os pagamentos realizados no equipamento passam a ser creditados na conta do golpista.

Dicas de prevenção

- Não deixar a maquineta em local de fácil acesso ao público e longe dos responsáveis pelo estabelecimento.
- Orientar os funcionários sobre a existência desse tipo de delito, a fim de mostrar a importância da vigilância constante dos equipamentos.
- Inserir etiqueta ou outra marcação que identifique o aparelho.
- Verificar, ao final do dia, se houve alteração nas características do instrumento, além de conferir se os valores estão sendo recebidos corretamente.

Golpe da assistência técnica

A fraude tem início quando criminosos enviam mensagens pela Internet informando que o computador que está sendo utilizado apresenta problemas ou está com o processamento lento. Em seguida, solicitam que o usuário baixe determinado aplicativo, que, na verdade, é uma ferramenta para roubar informações pessoais e financeiras das vítimas. Esse contato pode ser realizado por telefone, e-mail, sites que abrem sozinhos ou pop ups.

Dicas de prevenção

- Manter antivírus e firewalls atualizados.
- Evitar baixar programas desconhecidos.
- Atentar para o fato de que grandes empresas não enviam e-mails ou fazem ligações telefônicas solicitando informações pessoais ou financeiras.

Não acessar sites, links duvidosos ou emails suspeitos.

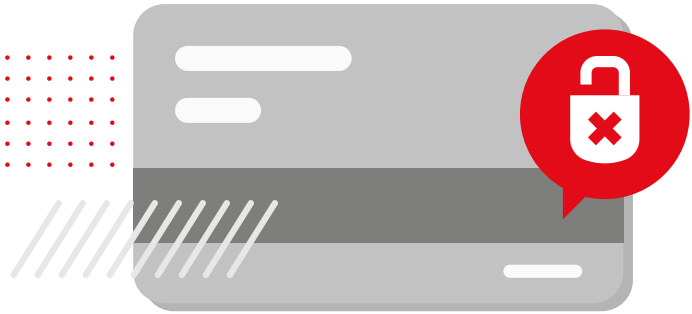
Furto de dados de cartão

O golpista utiliza-se de um descuido para colher informações pessoais que podem ser usadas para cometer fraudes. No momento em que se vai efetuar o pagamento de alguma compra cartão, o lojista, entregador ou prestador de serviço filma com seu celular os dados bancários contidos no cartão do cliente, inclusive o Código de Segurança. Com essas informações, o estelionatário tem a possibilidade de conseguir efetuar compras pela Internet utilizando os dados do cliente.

Dicas de prevenção

- Cobrir com fita adesiva o Código de Segurança dos cartões de crédito/débito.
- Manter rigorosa atenção durante o manuseio do cartão, não permitindo que o entregador, vendedor, atendente ou prestador do serviço leve o cartão para algum lugar sem sua supervisão.
- Em compras pela Internet, verificar se o site tem os selos de ambiente seguro.
- Se perceber que houve fraude, comunicar imediatamente à Central de Atendimento da operadora do cartão, solicitando seu bloqueio, e também gerar um Boletim de Ocorrência.

- Guardar com cuidado o cartão para não correr o risco de perdê-lo e nunca emprestar o cartão de crédito para terceiros.
- Verificar suas transações por meio de aplicativos para smartphones e acesso à internet banking diária ou semanalmente.
- Não acessar sites, links duvidosos ou emails suspeitos.
- 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.



Orientações gerais

Precauções

Esta cartilha virtual apresentou 46 estratégias utilizadas por criminosos que se aproveitam da boa fé das pessoas para obterem recursos de forma fraudulenta, gerando sérios prejuízos às vítimas. Há ainda inúmeras modalidades além destas apresentadas, que são algumas das mais praticadas atualmente.

Ressaltamos algumas das principais atitudes de segurança:

- Não acessar emails desconhecidos ou links suspeitos, uma vez que correspondem, em sua maioria, à porta de entrada para os criminosos terem acesso a dados e até mesmo senhas pessoais.
- Não aceitar ajuda de estranhos em bancos ou casas lotéricas. O aconselhável é sempre se dirigir a algum funcionário do estabelecimento financeiro.
- Não fornecer dados pessoais por mensagens de texto, aplicativos de mensagem ou ligação telefônica para estranhos. Tente se dirigir pessoalmente à agência bancária em casos de dúvidas ou necessidades.
- Não existe dinheiro fácil, seja prudente ao tratar de assuntos financeiros.
- Atenção com a documentação pessoal.
- Nunca guardar cartão e senha no mesmo local além de evitar empregar senhas ligadas a dados pessoais como datas de aniversário, etc.

- Manter as ferramentas de proteção digital atualizadas (antivírus, *firewall*, etc).
- Manter ativado o mecanismo de *Ativação em Duas Etapas* no aplicativo WhatsApp.
- Não depositar valores em contas de estranhos.

Caiu em um golpe? Veja algumas atitudes a serem tomadas.

Se perceber que caiu em um golpe, é muito importante adotar algumas medidas imediatamente. Veja a seguir algumas atitudes que podem ser tomadas:

- Comunicar o fato à instituição bancária e/ou à operadora do cartão da vítima.
- Trocar todas as senhas (emails, redes sociais, aplicativos) para ajudar a minimizar os danos.
- Reportar o golpe às autoridades competentes:
- O site da Secretaria de Defesa Social possui um link que encaminha o usuário à Delegacia Interativa, onde pode ser registrado o Boletim de Ocorrência On-Line. Em Pernambuco, a Polícia Civil dispõe da Delegacia especializada em crimes digitais: Delegacia de Polícia de Repressão aos Crimes Cibernéticos (DPCRICI).

- Avisar a todos os familiares e amigos de sua rede de relacionamento, orientando que ignorem qualquer tentativa de contato estranho, sobretudo se solicitarem alguma quantia em dinheiro.
- Informar a operadora de telefonia celular bem como o suporte do aplicativo, para que procedam com suas próprias medidas de segurança.

Contatos para denúncias

Polícia Militar 190

Delegacia de Polícia de Repressão aos Crimes Cibernéticos
Rua Gervásio Pires, 863 - Santo Amaro, Recife – PE
Fones: (81) 3184.3207/81 - 9.9488.7365

Delegacia Interativa SDS
https://servicos.sds.pe.gov.br/delegacia/

Procon Pernambuco
Rua Marquês do Herval, 141. Fone: 0800 282 1512

Delegacia do Consumidor Av. Conde da Boa Vista, 1410,
Boa Vista, Recife-PE. Fone: (81) 3184.3834

Assistência Militar e Policial Civil do MPPE
(Para situações que envolvam membro ou servidor do MPPE)
Fones: (81) 9.9969.9364 (Whatsapp)
Email: amsi@mppe.mp.br

Fontes de pesquisa

Guia de Orientação e Prevenção a Golpes, Exército Brasileiro, fevereiro de 2021.

"'Fraudes românticas' cresceram 31% durante a pandemia" Tecmundo. 22 de Fevereiro de 2021. Disponível em https://www.tecmundo.com.br/seguranca/211446-fraudes-romanticas-cresceram-31-eua-durante-pandemia.htm Acesso em 06 de maio de 2021.

"Caixa alerta para novo golpe". ContMoura, 21 de Janeiro de 2021. Disponível em https://contmoura.com.br/caixa-alerta-para-novo-golpe/ Acesso em 04 de maio de 2021.

Beneficiário do Auxílio Emergencial deve atualizar Caixa Tem, veja calendário. Agora Folha Uol, 10 de Março de 2021. Disponível https://agora.folha.uol.com.br/grana/2021/03/beneficiario-do-auxilio-emergencial-deve-atualizar-aplicativo-caixa-tem.shtml Acesso em 15 de abril de 2021.

"Polícia Civil alerta idosos sobre o 'golpe da baluda' e do 'falso bilhete premiado'". Governo do Estado do Amazonas. 22 de Julho de 2016. Disponível em http://www.amazonas.am.gov.br/2016/07/policia-civil-alerta-idosos-sobre-o-golpe-da-baluda-e-do-falso-bilhete-premiado/ Visualizado em 28 de abril de 2021.

"Dicas de segurança contra fraudes. Safra. Disponível em https://www.safra.com.br/dicas-de-seguranca-contra-fraudes.htm Acesso em 28 de abril de 2021.

"Cadastro de chaves do PIX é alvo de golpistas, alerta Febraban" Tecmundo 21 de Outubro de 2020. Disponível em https://www.tecmundo.com.br/seguranca/205623-cadastro-chaves-pix-alvo-golpistas-alerta-febraban.htm Acesso em 06 de maio de 2021.

"Conheça 8 golpes comuns aplicados por criminosos – por telefone e pessoalmente" Família. Disponível em https://www.familia.com.br/conheca-8-golpes-comuns-aplicados-por-criminosos-por-telefone-e-pessoalmente/ Acesso em 04 de maio de 2021.

"Portaria de Edifício e o Descuido que Facilita Assalto" Kênio Pereira Sociedade de Advogados. 18 de Fevereiro de 2019. Disponível em http://www.keniopereiraadvogados.com.br/Ver-Mais-1944#:~:text=Assaltantes%20e%20ladr%C3%B5es%20desenvolveram%20a,mesmo%20ao%20atender%20o%20interfone. Acesso em 31 de maio de 2021.

"Cartão de crédito clonado: o que fazer e como evitar?". Compara, 14 de Maio de 2019. Disponível em https://www.comparaonline.com.br/blog/financas/cartao-credito-clonado-devo/ Acesso em 27 de abril de 2021.

"Golpes financeiros explodem durante pandemia: veja quais são e como se prevenir" CNN Brasil. 24 de Março de 2021. Disponível em https://www.cnnbrasil.com.br/business/2021/03/24/golpes-financeiros-explodem-durante-pandemia-veja-quais-sao-e-como-se-prevenir Acesso em 04 de maio de 2021.

"Veja quais são os golpes mais comuns no WhatsApp e como se proteger" BBC News Brasil. 10 de Novembro de 2019. Disponível em https://www.bbc.com/portuguese/geral-50294962 Acesso em 07 de maio de 2021.

Mais de 15 mil pessoas têm WhatsApp clonado por dia no Brasil. IstoÉ Dinheiro, 16 de Outubro de 2020. Disponível em https://www.istoedinheiro.com.br/mais-de-15-mil-pessoas-tem-whatsapp-clonado-por-dia-no-brasil/ Acesso em 15 de Abril de 2021. Guia de Orientação e Prevenção a Golpes, Exército Brasileiro, fevereiro de 2021.

"50 golpes comuns no dia a dia" 08 de Fevereiro de 2013. Blog do Marcos Assi. Disponível em https://www.marcosassi.com.br/50-golpes-comuns-no-dia-a-dia Acesso em 28 de Abril de 2021. Guia de Orientação e Prevenção a Golpes, Exército Brasileiro, fevereiro de 2021.

"Crime cria nova tática de golpe por telefone" Folha de São Paulo. Disponível em https://www1.folha.uol.com.br/folha/cotidiano/ult95u115333.shtml Acesso em 05 de maio de 2021.

"Golpe promete 'dinheiro em dobro' após transferência com Pix, entenda". Canaltech, 18 de Janeiro de 2021. Disponível em https://canaltech.com.br/seguranca/golpe-promete-dinheiro-em-dobro-apos-transferencia-com-pix-entenda-177569/ Acesso em 23 de abril de 2021.

14 cuidados para evitar golpes com documentos pessoais e cheques. Infomoney, 31 de Maio de 2013. Disponível em https://www.infomoney.com.br/minhas-financas/14-cuidados-para-evitar-golpes-com-documentos-pessoais-e-cheques/ Acesso em 15 de abril de 2021.

"Alerta sobre golpe de crédito consignado" APFUSC Sindical. 30 de Março de 2021. Disponível em https://www.apufsc.org.br/2021/03/30/alerta-sobre-golpe-de-credito-consignado/ Acesso em 04 de maio de 2021

"Engenharia Social: a arte de enganar" OSTEC. Disponível em https://ostec.blog/geral/engenharia-social-a-arte-de-enganar/ Acesso em 04 de maio de 2021.

"Conheça os 10 golpes mais aplicados por estelionatários" Jusbrasil. Há 5 anos. Disponível em https://laiannecst.jusbrasil.com.br/noticias/376203723/conheca-os-10-golpes-mais-aplicados-por-estelionatarios Acesso em 06 de maio de 2021.

"Por detalhes, Alegretense não cai no 'Golpe dos Nudes'" Alegrete Tudo, 03 de Outubro de 2020. Disponível em https://www.alegretetudo.com.br/por-detalhes-alegretense-nao-cai-no-golpe-dos-nudes/ Acesso em 27 de abril de 2021

"Mensagem sobre "falsa multa do Detran" é real? Comprova, Revide!" Revista Revide. 13 de Agosto de 2019. Disponível em https://www.revide.com.br/comprova-revide/mensagem-sobre-falsa-multa-do-detran-comprova-revide3/. Visualizado em 28 de abril de 2021.

"O novo golpe por transferências no Pix via Whatsapp e do 'falso empréstimo'." Migalhas.com, 14 de Abril de 2021. Disponível em https://www.migalhas.com.br/depeso/343685/o-novo-golpe-por-transferencias-no-pix-via-whatsapp Acesso em 23 de abril de 2021.

"Leilões de Imóveis Falsos: Fique Atento!" Zukerman Blog, 06 de Março de 2020. Disponível em https://www.zukerman.com.br/blog/fique-atento-aos-falsos-sites-de-leilao-de-imovel Acesso em 29 de abril de 2021.

"Mulher é vítima do golpe do falso sequestro em Major Vieira." 9 de dezembro de 2020.

Jornalismo Digital. Disponível em https://www.jmais.com.br/mulher-e-vitima-do-golpe-do-falso-sequestro-em-major-vieira/ Acesso em 23 de abril de 2021.

"Criminosos aplicam golpes em famílias com parentes internados em hospitais" CEMIG Saúde. Disponível em https://www.cemigsaude.org.br/site/pagina/detalhe/13792 Acesso em 04 de maio de 2021.

Bandidos roubam fotos do WhatsApp para dar golpe. Veja como se proteger." Midia Hoje. 30 de Setembro de 2020. Disponível em https://www.midiahoje.com.br/geral/bandidos-roubam-fotos-do-whatsapp-para-dar-golpe-veja-como-se-proteger/6779 Acesso em 07 de maio de 2021.

"Grupo é detido suspeito de aplicar golpe em estudantes de Foz do Iguaçu" G1. Disponível em https://g1.globo.com/pr/oeste-sudoeste/noticia/grupo-e-detido-suspeito-de-aplicar-golpe-em-estudantes-de-foz-do-iguacu.ghtml Acesso em 05 de maio de 2021.

VÍDEO: Procon faz alerta de novo golpe de celular que acessa dados em 10 segundos. OCNET. Disponível em http://www.ocnet.com.br/noticias/blog-do-giu/video-procon-faz-alerta-de-novo-golpe-de-celular-que-acessa-dados-em-10-segundos/ Acesso em 04 de maio de 2021.

Fontes: "Gastos no cartão de crédito de vítima de 'golpe do motoboy' são inexigíveis, decide Justiça". Tribunal de Justiça do Estado de São Paulo. 01 de Outubro de 2020. Disponível em https://www.tjsp.jus.br/Noticias/Noticia?codigoNoticia=62349 Acesso em 26 de abril de 2021.

"Os seis principais golpes on-line: como não se tornar uma vítima". Kaspersky. Disponível em https://www.kaspersky.com.br/resource-center/threats/top-six-online-scams-how-to-avoid--becoming-a-victim Acesso em 27 de abril de 2021.

"Conheça os golpes que são mais aplicados em aposentados"- Folha BV. 05 de Fevereiro de 2020. Disponível em https://folhabv.com.br/noticia/CIDADES/Capital/Conheca-os-golpes-que-mais--sao-aplicados-em-aposentados/62427 Acesso em 29 de abril de 2021.

"Delegado alerta para o golpe da passagem aérea. Portal Menina, 08 de Outubro de 2020. Disponível em https://portalmenina.com.br/balneario-camboriu/2020/10/08/delegado-alerta-para--o-golpe-da-passagem-aerea/ Acesso em 29 de abril de 2021.

"Golpe do pecúlio está sendo aplicado novamente: aposentados são vítimas de estelionatários."Camprev Campinas SP, 09 de Fevereiro de 2021. Disponível em https://camprev.campinas.sp.gov.br/golpe-peculio-sendo-aplicado-novamente-aposentados-sao-vitimas-estelionatarios. Acesso em 29 de abril de 2021.

"Dicas de TI: conheça e saiba como se proteger dos principais golpes praticados na internet" Steiner & Moura Ferro Advogados Associados. Disponível em http://steinermouraferro.com.br/noticia.php?id=10 Acesso em 04 de maio de 2021.

Fontes: "Golpe do falso email de banco aumenta 80% durante a pandemia, diz federação" Economia Uol. Disponível em https://economia.uol.com.br/noticias/redacao/2020/09/21/golpe--phishing-aumento-pandemia-coronavirus-febraban.htm Acesso em 05 de maio de 2021.

Fontes: "Ransomware Como Proteger seus dados"QNAP. Disponível em https://www.qnapbrasil.com.br/blog/post/ransomware-como-proteger-seus-dados Acesso em 29 de abril de 2021.

Guia de Orientação e Prevenção a Golpes, Exército Brasileiro, fevereiro de 2021.

"Pirâmide financeira: como evitar cair nesse golpe!" Xerpay. 09 de junho de 2020. Disponível em https://www.xerpa.com.br/blog/piramide-financeira/ Acesso em 06 de Maio de 2021.

"Alertas de Golpes e Fraudes" Petrobras Investidores. Disponível em https://www.investidorpetrobras.com.br/servicos-ao-investidor/alertas-de-golpes-e-fraudes-2/ Acesso em 06 de maio de 2021.

"Saiba como evitar golpes em sites de leilões falsos" Superbid Blog. Disponível em https://blog.superbid.net/saiba-como-evitar-golpes-em-sites-de-leiloes-falsos/ Acesso em 04 de maio de 2021.

"Black Friday: vítima de site falso não pode processar loja" R7. Disponível em https://noticias.r7.com/economia/black-friday-vitima-de-site-falso-nao-pode-processar-loja-24112017 Acesso em 04 de maio de 2021.

"Lojista, cuidado: o golpe da troca da máquina de cartão" Jusbrasil. Disponível em https://canalcienciascriminais.jusbrasil.com.br/artigos/641752463/lojista-cuidado-o-golpe-da-troca-da-maquina-de-cartao Acesso em 31 de maio de 2021.

"Criminosos usam vales-presente falsos para roubar dados e infectar aparelhos" Segurança Uol. Disponível em https://se-

guranca.uol.com.br/antivirus/dicas/curiosidades/criminosos_usam_vales_presente_falsos_para_roubar_dados_e_infectar_aparelhos.html#rmcl Acesso em 04 de maio de 2021.

MP PE
Ministério Público de Pernambuco
CONECTADO COM A INCLUSÃO

MINISTÉRIO PÚBLICO DE PERNAMBUCO
Rua do Imperador D. Pedro II, 473, Edf. Promotor de Justiça Roberto Lyra,
Santo Antônio, Recife, PE – CEP: 50010-240, Tel (81) 3182.7000 - www.mppe.mp.br

MP PE

Ministério Público de Pernambuco

CONECTADO COM A INCLUSÃO