CARTILHA DE PREVENÇÃO CONTRA GOLPES

2021

ARGOS

SUMÁRIO

1. OBJETIVO 3
2. INTRODUÇÃO 3
3. GOLPES COM A CÓPIA DE DOCUMENTAÇÃO PESSOAL 3
4. FALSO SEQUESTRO 4
5. CLONAGEM DE CARTÃO DE CRÉDITO 4
6. FALSO FUNCIONÁRIO DO BANCO 5
7. GOLPE DO BILHETE PREMIADO 6
8. GOLPE DA PASSAGEM AÉREA 6
9. GOLPE EM SITES DE COMÉRCIO ELETRÔNICO 7
10. GOLPE DE SITES “FAKE” 7
11. PHARMING 8
12. ENGENHARIA SOCIAL 8
13. PHISHING 9
14. GOLPE DA PIRÂMIDE 10
15. PENDÊNCIAS JUNTO AOS ÓRGÃOS DE PROTEÇÃO DE CRÉDITO 10
16. GOLPE DO EMPRÉSTIMO CONSIGNADO 11
17. CLONAGEM DO NÚMERO DO CELULAR 11
18. GOLPE DE FAMILIAR INTERNADO 12
19. GOLPE SOBRE O PARENTE COM DIFICULDADE 12
20. GOLPE DA AÇÃO JUDICIAL OU PECÚLIO 13
21. GOLPE DA “BATIDINHA” NO TRÂNSITO 13
22. GOLPE DA “SEXTORSÃO” 14
23. GOLPES ENVOLVENDO PIX 15
24. GOLPE DA VACINAÇÃO DA COVID - 19 15
25. SEQUESTRO DE DADOS 16
26. CLONAGEM DE WHATSAPP 17

1. OBJETIVO

Esta cartilha tem por objetivo apresentar golpes comumente praticados em nossa sociedade, bem como as formas de identificar e se prevenir contra a ação de criminosos que se utilizam desses métodos.

2. INTRODUÇÃO

Diversos golpes são aplicados por criminosos em indivíduos da nossa sociedade e com maior incidência sobre indivíduos idosos. Os recentes vazamentos de dados de cidadãos brasileiros, faz com que seja mais fácil a continuidade dessas práticas.

De forma geral, os meliantes mostram conhecimento sobre dados pessoais relevantes da vítima e de seus familiares ou pessoas próximas. Essas informações podem ter sido coletadas através de vazamento de dados ou coletados através de engenharia social, o que facilita a ação de golpistas.

Os golpes têm maior chance de êxito se o golpista obtiver sucesso em explorar as seguintes fragilidades:

1. A falta de informação da vítima;

2. A ambição da vítima por algum ganho pessoal.

Sendo assim, este Guia tem por finalidade alertar e orientar os indivíduos quanto as mais diversas formas de golpes, assim como formar de salvaguardar a segurança pessoal.

3. GOLPES COM A CÓPIA DE DOCUMENTAÇÃO PESSOAL

Esses golpes são aplicados utilizando-se de uma cópia de algum documento pessoal da vítima.

Na maior parte das vezes instituições ou estabelecimentos comerciais que concedem crédito solicitam uma cópia de alguns documentos como, por exemplo, identidade e CPF.

Nessas situações, a cópia do documento da vítima pode ser extraviada ou furtada, para ser usada por golpistas para fins indevidos, como realizar solicitação de empréstimos em instituições bancárias, confecção de documentos falsos, etc.

Dica de Prevenção:

- Quando tiver que entregar alguma cópia de documento em algum estabelecimento, insira as linhas sobre o documento e escreva a finalidade daquela cópia.

4. FALSO SEQUESTRO

Nessa modalidade de golpes o falso sequestrador segue os seguintes passos:

- Telefona para vítima e diz que sequestrou algum parente ou pessoa próxima;
- Exige que uma quantia seja depositada em uma conta-corrente por ele indicada, para pagar pelo resgate;
- Proíbe a vítima de interromper a ligação.

Obs.: Em casos de sequestros reais, o sequestrador não impede a vítima de interromper a ligação.

Dicas de prevenção:

- Sempre orientar as pessoas da casa a não fornecerem dados pessoais, por telefone ou através de redes sociais. Pois, essas informações que os criminosos usam para dar maior credibilidade aos golpes;
- Antes de qualquer ação, procure a ajuda de alguém que não esteja envolvido emocionalmente com o caso;
- Tente contato com a pessoa supostamente sequestrada.

5. CLONAGEM DE CARTÃO DE CRÉDITO

O golpista nesses casos trabalha em um estabelecimento comercial ou como motoboy, o marginal utiliza uma máquina leitora de cartão com mecanismo de cópia de dados, conhecida como "Chupa-Cabra".

No momento em que o alvo entrega o cartão para efetuar o pagamento, o golpista o insere nessa máquina e, depois que o cliente insere a senha, diz que

a máquina está com problema de acesso e passa o cartão em outra máquina, realizado assim o pagamento.

As informações do cartão são gravadas pela primeira máquina, até mesmo a senha da vítima, o que possibilita a clonagem do cartão para utilização para realização de compras e pagamento sem o conhecimento da vítima.

Obs.: Esse golpe também pode ocorrer em caixas eletrônicos, utilizando dispositivos para leitura do seu cartão.

Dicas de Prevenção:

- Se a máquina de cartão não funcionar e for necessária a troca, solicitar a presença do gerente do comércio e registrar a ocorrência para se for necessário, registrar em uma delegacia;
- Cadastrar o seu número móvel junto ao banco, para receber SMS avisado sobre todos os movimentos financeiros na conta bancária ou do cartão de débito, ou crédito.

6. FALSO FUNCIONÁRIO DO BANCO

Nas agências bancárias, em filas de caixas eletrônicos, especialmente nos destinados a depósitos, o golpista se passar por funcionário da agência e organiza a fila de espera dos clientes.

No momento seguinte, recolhe os envelopes de depósito com dinheiro, solicitando que aguardem o recibo por alguns instantes, saindo rapidamente do local, levando o dinheiro das vítimas.

Dicas de Prevenção:

- Manter sigilo sobre senha da conta;
- Não aceitar ajuda de estranhos em filas de agências bancárias;
- Caso precise de ajuda, confirme quem é o funcionário do banco que está à disposição.

7. GOLPE DO BILHETE PREMIADO

O golpista aborta da vítima nada rua, trajando roupas simples e dizendo ser de fora da cidade, afirma estar de posse de um bilhete de loteria premiado, contudo tem que viajar imediatamente, dessa maneira, estando impossibilitado de aguardar para resgatar o prêmio.

Usando dessa história, criminoso procura convencer a vítima a comprar o bilhete.

Obs.: Em alguns casos existe a promessa de divisão do prêmio entre a vítima e o golpista, que após receber o depósito da vítima, desaparece.

Dicas de prevenção:

- Lembrar que "não existe almoço grátis", ou seja, não existe dinheiro fácil;
- Sempre desconfiar de pessoas estranhas com ofertas demasiadamente generosas.

8. GOLPE DA PASSAGEM AÉREA

Nessa modalidade de golpe o estelionatário vende uma passagem aérea por um preço muito abaixo do praticado pelo mercado, sob a alegação de se tratar de um bônus de cartão de milhagem.

A vítima compra a passagem e quando vai embarcar, ocasião em que a identidade é solicitada, é informada que a passagem foi adquirida de forma ilícita, sendo assim, impedida de realizar a viagem e acaba senso acusada de conluio no golpe.

Dicas de Prevenção:

- Não aceitar ofertas muito vantajosas vinda de pessoas estranhas.
- Comprar passagens apenas de companhias aéreas, agências de turismo e sites de pacotes de viagens comprovadamente legais.

9. GOLPE EM SITES DE COMÉRCIO ELETRÔNICO

O meliante, se passa por comprador ou por vendedor, agindo de má-fé e não cumpre com o acordo ou se utiliza dos dados pessoais e financeiros dos envolvidos na transação para fins indevidos.

Obs.: É comum o envio de falsos e-mails, simulando o sistema de gerenciamento de pagamento, como maneira de comprovar a realização de pagamento ou envio de mercadoria, o que na realidade, não foi feito.

Dicas de Prevenção:

- Faça uma pesquisa para identificar se um produto está muito abaixo do preço de mercado;
- Verificar sempre o endereço de e-mail de e-mails recebidos, referentes a assunto comerciais ou financeiros, pois podem ser facilmente falsificados.
- Sempre acesse os sites diretamente pelo navegador evitando abrir links enviados por mensagens;
- De preferência a realizar pagamentos pessoalmente, por meio de boletos;
- Quando for realizar compras online de preferência a sites de comércio eletrônico conhecidos.

10. GOLPE DE SITES “FAKE”

O criminoso cria um site "fake" a fim de que vítima(s), realize compras e realize o pagamento, porém após o pagamento ser efetuado a vítima não recebe o produto.

As ofertas desses sites "fakes", são comumente enviadas por e-mail spam, mensagens de WhatsApp, propagandas via links patrocinados e sites de compras coletivas e com preços muito abaixo dos praticados no mercado.

Dicas de Prevenção:

- Procure conhecer a reputação do site em sites de avaliação como: ReclameAqui;

- Cuidado com promoções recebidas por meio de spam;
- Busque informação sobre os dados de cadastro da empresa no site da Receita Federal;
- Sempre compare os preços em outros sites para saber se o desconto oferecido está fora do padrão que é praticado no mercado.

11. PHARMING

Esse tipo de prática se dá pelo redirecionamento da navegação do usuário para sites falsos. Isso ocorre quando a vítima tenta acessar um site legítimo, porém o seu navegador é redirecionado para uma página falsa.

Essa modalidade de golpe é muito comum quando se está tentando acessar o internet banking.

Dicas de Prevenção:

- Sempre desconfie de sites que sugiram abrir algum arquivo ou solicitem a instalação de algum programa;
- Sempre que estiver acessando um site de compras ou internet banking, verifique se está em uma conexão segura. É possível fazer essa verificação através da sigla *"https"* exibida antes do endereço do site;
- Verificar se o certificado apresentado corresponde ao do site verdadeiro.

12. ENGENHARIA SOCIAL

Os Golpistas se aproveitam de fragilidades pessoais, desconhecimento e despreocupação quanto a medidas de segurança pessoal, por parte das vítimas.

São utilizadas técnicas de engenharia social, os meios e discursos são variados, procurando persuadir e enganar a vítima a executarem ações que exponham suas informações sensíveis.

Após coletar essas informações, o meliante as utiliza de forma indevida, para acessar sites, enviar mensagens, criar empresas fantasmas, falsas contas bancárias e efetuar transações financeiras.

Dicas de Prevenção:

- Tenha muita atenção ao compartilhar dados pessoais, ainda que seja com pessoas que você conheça. Busque saber, sempre o motivo da solicitação dessas informações e se elas são realmente relevantes para o assunto em questão.

13. PHISHING

Nessa modalidade de golpe o contato com a vítima, quase sempre, é realizado por e-mail fingindo ser de alguma companhia conhecida.

No momento em que o alvo clica em algum link ou abre algum arquivo executável, do e-mail, é instalado no computador da vítima um Trojan, conhecido como Cavalo de Tróia.

O Cavalo de Tróia é capaz de capturar suas informações pessoais e até mesmo alterar o endereço de destino do provedor de internet.

Dicas de Prevenção:

- Tenha atenção a e-mails com links para baixar e (ou) executar arquivos;
- Atenção a mensagens eletrônicas com formulários para preenchimento de dados pessoais e financeiros;
- É comum que o criminoso que se utiliza desses golpes use e-mails de aviso judicial, promoções de programa de milhagem de companhias aéreas, álbuns de fotos ou vídeos, serviços de proteção de crédito e da Receita Federal, por isso muita atenção ao receber e-mails com esse tipo de conteúdo.

14. GOLPE DA PIRÂMIDE

O golpe da pirâmide é baseado em um sistema de fraudes usado para coletar dinheiro ou benefícios por meio de um fluxo supostamente "inesgotável", de novos participantes.

Cada novato na pirâmide tem a função de dar dinheiro para os "recrutadores" e recrutar novos participantes para o esquema.

Dicas de Prevenção:

- Lembre-se dinheiro fácil não existe, desconfie de pessoas oferecendo retorno financeiro com pouco/nenhum esforço.

Obs.: Esquemas de pirâmide são crimes contra e economia popular e está previsto no Art. 2º, IX da Lei Nr° 1.521/51.

15. PENDÊNCIAS JUNTO AOS ÓRGÃOS DE PROTEÇÃO DE CRÉDITO

O golpista envia uma correspondência, e-mail ou realiza uma ligação para vítima informado que a mesma está negativada com os órgãos de proteção ao crédito e que possui alguma pendência com alguma instituição bancária ou órgão do governo que foi que registrada em cartório.

Após o primeiro contato, ou mesmo no primeiro contato, é enviado um boleto para pagamento que quitaria a suposta dívida.

Dica de Prevenção:

- Confirme com o banco e órgãos de proteção ao crédito (por canais oficiais), toda a informação que foi recebida através, do e-mail, correspondência ou ligação.

16. GOLPE DO EMPRÉSTIMO CONSIGNADO

A vítima recebe uma ligação de um estelionatário afirmando ser um representante de uma entidade financeira, oferecendo um empréstimo com juros menores. Mas para isso, solicita o identificador consignável do contracheque da vítima.

Após esse primeiro procedimento, é realizado o depósito de um valor considerável na conta-corrente da vítima. Em um novo momento, o golpista liga novamente para vítima informando que o valor depositado se tratava de um equívoco e solicita a devolução de parte do valor em uma conta-corrente por ele indicada.

No mês posterior aos fatos, a vítima é surpreendida com o desconto em contracheque da 1ª parcela de empréstimo (feito em seu nome prelo criminoso de posse de seus dados e do identificador consignável).

Dicas de Prevenção:

- Desconfie de empréstimos com juros muito vantajosos;
- Não informe seus dados por telefone;
- Desconfie de qualquer depósito, não programado, em sua conta;
- Procure seu Gerente de Conta.

17. CLONAGEM DO NÚMERO DO CELULAR

O golpista se passando por funcionário de uma empresa de telefonia, liga para o número móvel da vítima dizendo que foi detectado um defeito naquele aparelho e solicita que digite um número fornecido por ele.

A partir dessa ação o marginal clona o número da linha e a utiliza de formas indevidas, realizando o todo tipo de ligação a níveis regionais, nacionais e internacionais.

Dicas de Prevenção:

- As empresas de telefonia nunca ligam para os celulares de seus clientes solicitando que sejam digitados números no aparelho, sob o pretexto de solucionar possíveis falhas ou defeitos.

18. GOLPE DE FAMILIAR INTERNADO

A vítima recebe a ligação, de um golpista, sobre um familiar que está internado em algum hospital. O golpista se passa por um profissional de saúde, diz é necessário a liberação de exame ou de uma cirurgia urgente, e para que o procedimento seja realizado e preciso que façam um depósito bancário na conta por ele indicada.

Após a realização do depósito o golpista transfere ou saca o dinheiro e desaparece.

Dicas de Prevenção:

- Caso receba esse tipo de ligação, entre em contato com a administração ou ouvidoria do hospital para se certificar de que não está sendo vítima de um golpe.

19. GOLPE SOBRE O PARENTE COM DIFICULDADE

Nesse tipo de golpe, o criminoso entra em contato com o alvo e se passa por um parente que está tendo problemas, na grande maioria das vezes se trata de problemas financeiros.

Em uma nova ligação, o golpista solicita que a vítima deposite uma quantia, em dinheiro, para socorrê-lo e que assim que possível retornará o valor. Assim que é feito o depósito as ligações cessam e o golpista desaparece, não sendo possível contactá-lo pelo número que utilizado para realizar as ligações.

Dicas de Prevenção:

- Após a primeira ligação, ligue para o número registrado em sua agenda da pessoa;
- Não deposite dinheiro na conta de desconhecidos;
- De preferência para tratar de assuntos financeiros presencialmente.

20. GOLPE DA AÇÃO JUDICIAL OU PECÚLIO

O criminoso, e passando por um funcionário de associação, empresa de previdência privada, advogado ou representante jurídico, entra em contato com a vítima informando sobre um suposto valor de pecúlio ou valos a receber de uma ação judicial coletiva e oferecendo o saque imediato.

Para isso, tudo o que a vítima precisa fazer é depositar, em uma conta indicada pelo golpista, uma quantia correspondente aos custos administrativos ou processuais.

Após esse depósito e estando de posse dos dados pessoais e bancários da vítima, o criminoso deposita na conta-corrente um cheque furtado, roubado ou sem fundo, que fica bloqueado por mais de 24 horas de depois é suspenso.

Dicas de Prevenção:

- Nunca forneça ou confirme seus dados a estranho. Caso precise tratar de questões financeiras procure instituições credenciadas e dê preferência a fazê-lo pessoalmente
- A prática judicial não prevê ligações para comunicar êxito em ações na justiça, por isso muito cuidado ao receber esse tipo de ligação.

21. GOLPE DA "BATIDINHA" NO TRÂNSITO

Nessa situação os criminosos, dirigindo um carro normalmente roubado, encostam atrás do carro da vítima simulando uma pequena batida, com o intuito de pará-la.

A vítima por sua vez para o veículo para analisar o dano e conversar com o outro condutor, nesse momento é anunciado o roubo e a vítima tem seus pertences e veículo roubados.

Obs 1.: Os criminosos priorizam esse tipo de prática em locais isolados.

Obs 2.: A maioria das vítimas são mulheres.

Obs 3.: Carros de luxo são os mais visados.

Dicas de Prevenção:

- Sempre informe a alguém de confiança o trajeto e sua localização;
- Se o lugar onde a batida ocorrer for deserto e dependendo do dano causado, siga viagem. É melhor um pequeno prejuízo do que pôr em risco a sua vida;
- Pare apenas em locais seguros, com algum tipo de vigilância ou movimentação constante.

22. GOLPE DA "SEXTORSÃO"

Nesses casos o golpista aborda a vítima através das mídias sociais para iniciar uma amizade através de troca de mensagens. Depois de ganhar a confiança da vítima as conversas ficam mais picantes e o farsante solicita imagens e vídeos íntimos da vítima.

A vítima, por sua vez, envolvida com a evolução das conversas, acaba cedendo e enviando fotos e vídeos. E a partir desse momento começam as ameaças ou chantagens para que as fotos ou vídeos não sejam divulgados na internet.

Dicas de Prevenção

- Recuse pedidos de amizade ou mensagens de pessoas desconhecidas;
- Não compartilhe fotos e vídeos íntimos em redes sociais;
- Evite armazenar fotos e vídeos em seu celular, notebook ou computador. Esses conteúdos podem acabar sendo expostos se o aparelho for hackeado ou até mesmo quando forem deixados para manutenção.
- Evite chamadas de vídeo com desconhecidos;
- Caso se torne uma vítima dessa prática, não apague as conversas e procure a Polícia para registrar a ocorrência.

23. GOLPES ENVOLVENDO PIX

O Pix é a nova modalidade de pagamento e transferência de valores criada pelo Banco Centra, que garante maior agilidade em transações financeiras por canais eletrônicos de instituições financeiras.

Com isso mais uma vez, os criminosos se adaptaram e criaram golpes envolvendo as transações realizadas por PIX.

Na maior parte desses golpes a vítima recebe um link por SMS, E-mail ou redes sociais com ofertas de cadastro no serviço de pagamento PIX, que podem conter Malwares ou direcionar para sites falsos.

Clicando nesses links a vítima acaba por expor informações pessoas e financeiras para o criminoso, que passa a utilizar-se dessas informações para atos ilícitos.

Dicas de Prevenção:

- Nunca realize o seu cadastro por meio de algum link recebido por SMS, E-mail ou WhatsApp;
- Não informe a ninguém algum código fornecido por SMS ou por QR Code;
- Verifique se o QR Code recebido está apontado para o endereço correto para pagamento antes de inserir a chave de autorização PIX;
- Certifique-se de estar logado no site ou aplicativo oficial do seu banco antes de realizar transações financeiras por meio eletrônico;
- - Em caso de dúvidas sobre o PIX entre em contato com seu banco ou acesse as informações disponíveis no site do Banco Central.

24. GOLPE DA VACINAÇÃO DA COVID - 19

O Golpista liga para a vítima se identificando como agente do Ministério da Saúde ou alguma instituição de saúde local e oferece um pré-cadastro para vacinação, com objetivo de obter dados pessoais da vítima.

Em outra modalidade o criminoso encaminha uma mensagem de texto, por WhastApp ou SMS, com um link ou código para um falso cadastro, que pode levar à clonagem do WhastApp da vítima.

Devido a atual situação, a vítima acreditando se tratar de um contato verdadeiro acaba fornecendo os dados pessoais.

Dicas de Prevenção:

- Em hipótese alguma forneça dados pessoais por meio de ligação ou link recebido;
- Procure os órgãos oficiais para mais informações sobre a vacinação;
- Mesmo que indicados por conhecidos, não acesse links suspeitos;
- Utilize os mecanismos de segurança em duas etapas de seus aplicativos e e-mail;
- Caso receba um link ou ligação suspeita denuncie às entidades oficiais e registre um B.O. em uma Delegacia.

25. SEQUESTRO DE DADOS

Para realiza esse golpe, o criminoso invade e instala um programa malicioso chamado "Ransonware", capaz de criptografar as informações armazenadas em um computador ou servidor corporativo.

Depois que os arquivos são criptografados, a vítima perde completamente o acesso às informações dos arquivos, pois ficam bloqueados.

Como condição de informar a chave para descriptografar o arquivo, os criminosos exigem o pagamento de um resgate em moeda digital (criptomoeda).

Obs.: Nem sempre as chaves liberadas pelos criminosos funcionam.

Dicas de Prevenção:

- Mantenha um Backup sempre atualizado dos arquivos do computado em um dispositivo externo (Hd externo ou pen drive) ou em um servidor preparado para isso;
- Não acesse sites suspeitos;
- Jamais acesse links ou e-mails duvidosos;
- Mantenha os firewalls e antivírus, do computador, ativos.

26. CLONAGEM DE WHATSAPP

Nesse golpe o criminoso se passado por um funcionário da operadora de telefonia, alguma loja ou site, diz que irá enviar um código promocional ou código de confirmação.

Depois pede que a vítima informe esse código que, na verdade, é código de verificação do WhastApp, dessa forma clonando a contada vítima, que perde completamente o acesso e o controle do mensageiro.

Além do prejuízo de perder a conta, a vítima com isso concede acesso aos dados armazenados como, por exemplo, contatos que passam a ser alvos de golpes financeiros.

Dicas de Prevenção:

- A primeira delas é que você sempre tenha a verificação em duas etapas, ativada no aplicativo;
- Nunca forneça códigos recebidos por SMS ou e-mail;
- Desconfie de solicitações de pagamentos ou transferências com urgência;
- Não instale aplicativos de terceiros não verificados;
- Caso seja uma vítima, informe seus contados para que não caiam em golpes, e registe um Boletim de Ocorrência.

CONTATO

Avenida das Américas, Nº 3434, Bloco 02, Sala 505 - Barra da Tijuca

Telefones: 21 2027-1320 / 21 99794-1097 (WhatsApp)

E-mail: contato@consultoriaargos.com.br

www.consultoriaargos.com.br