CARTILHA DE ORIENTAÇÕES

2022

FRAUDES E GOLPES DIGITAIS

Os riscos da evolução ciber-criminosa

CACB FACIAP CACIOPAR ACES SISTEMA ASSOCIATIVISTA

CACIOPAR COORDENADORIA DAS ASSOCIAÇÕES COMERCIAIS E EMPRESARIAS DO OESTE DO PARANÁ

CACB FACIAP CACIOPAR ACICAF SISTEMA ASSOCIATIVISTA

ACICAF

CONSEG Paraná

INFORMAÇÕES E CONTATO
Coordenadoria das Associações Comerciais e Empresariais do Oeste do Paraná – CACIOPAR
Rua Pernambuco, 1800, anexo à Acic – 1º andar – centro, Cascavel
Telefone: (45)3321-1449
www.caciopar.org.br

Associação Comercial e empresarial de Cafelândia – ACICAF
Rua Dr. Plinio Costa, nº 645, Centro, Cafelândia.
Telefone: (45) 3241-1360
www.acicaf.com.br

Conselho Comunitário de Segurança de Cafelândia – CONSEG
Rua Governador Moises Lupion, 760, Centro, Cafelândia, Anexo à Policia Militar
Telefone: (45) 9 9963-0193
Email: conseg.cafelandia@gmail.com

ORGANIZAÇÃO DO MATERIAL
Editor:
Thiago Camargo de Freitas, Policial Militar do Estado do Paraná, Presidente do CONSEG Cafelândia, Presidente do COMAD de Cafelândia, Graduado em Direito, Especialista em Segurança Pública, Especialista em Criminologia, Especialista em Investigação Forense e Perícia Criminal, Especialista em Direito Penal Militar e Processo Penal Militar, pós-graduando em Direitos Humanos e Ressocialização; pós-graduando em Ciências Criminais.

Co-editor:
Rivelino Skura, Advogado, Presidente da ACICAF, Secretário Geral da comissão de direito Público da OAB Cascavel, Procurador Público de Nova Cantu, Diretor da Microrregião 02 da CACIOPAR, Delegado da Cooperativa de Credito Sicredi; Membro do conselho POD – Programa Oeste em Desenvolvimento; Especialista em Direito Público, Especialista em Direito Civil e Processual Civil; Especialista em Direito do Estado.

Projeto Gráfico, Editoração Eletrônica e Revisão Ortográfica
Comunicação ACICAF

SUMÁRIO

INTRODUÇÃO AO CONTEÚDO

Nosso objetivo com esta cartilha é explorar alguns conceitos básicos sobre a ciber–criminologia, além de disseminar orientações sobre Fraudes que ocorrem no território da internet, vitimando milhões de pessoas o Brasil e causando prejuízos bilionários.

De forma bem ilustrativa e conteúdo objetivo, queremos que os leitores tenham uma base solida sobre o que são os crimes de Fraudes, golpes de internet, a forma que geralmente ocorrem, quais as maneiras de se manter seguro e o que fazer diante de um golpe cibernético.

Daremos o caminho mais eficiente para a prevenção e a reparação de danos causados quando diante de uma fraude cibernética.

Apos a leitura desta cartilha, com certeza você será capaz de entender, Orientar e previnir a vitimização de pessoas frente a fraudes que ocorrem diariamente no territorio do ciber-crime.

Mãos à obra e bom proveito!

EVOLUÇÃO HISTÓRICA DA CIBER-CRIMINOLOGIA

O advento da internet, principalmente em decorrência da evolução tecnológica das últimas décadas, que nos trouxe praticidades, em seu bojo carregou consigo vários problemas, pois ao mesmo tempo em que facilita as atividades e práticas econômicas e sociais, também, disso surgem as oportunidades criativas para cometimento de crimes que possam gerar, desde constrangimentos, prejudicar ou até mesmo difamar uma pessoa, a situações que geram consideráveis prejuízos financeiros.

Os primeiros programas que invadiam os computadores pessoais surgiram como “vírus”, e sua origem remonta o início da década de 70, sendo disseminados através de disquetes contaminados, alterando as informações ao iniciar o computador e com isso acessando conteúdos privados de pessoas e empresas com o intuito fraudulento.

Nem todas as ações criminosas se enquadram em legislações, tendo formas de execuções particulares a cada pratica criminosa, sendo necessário que as legislações que criminalizam estes crimes sejam mais especificas, principalmente no âmbito penal, pois algumas leis que sobre práticas ilícitas no âmbito cibernético estão previstos apenas na esfera civil, não ocorrendo punições que sejam capazes de efetivamente reparar os danos das vítimas, pois diversas condutas não estão tipificadas em leis criminais.

Nos primórdios da internet, tínhamos como crime cibernético apenas a pirataria de softwares e arquivos da internet. Com a evolução tecnológica e por consequência a chegada de conexões cada vez mais rápidas e de grande fluxo nas trocas de informações e conteúdos, expandiu-se a variedade de crimes praticados por meio dela.

Conceitua-se o crime de informática como sendo: *“A conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar”*

O QUE SÃO OS CIBER-CRIMES?

Segundo a legislação brasileira, definem-se como crimes cibernéticos, as ações criminosas que geram danos a indivíduos ou patrimônios, através da utilização de computadores, redes de computadores ou dispositivos eletrônicos conectados.

Os danos que decorrem dos crimes cibernéticos, podem ser causados através de extorsão de recursos financeiros, estresse emocional ou danos à reputação das vítimas expostas na Internet. Alguns exemplos típicos de crime virtual são:

1. Uso de dados financeiros ou credenciais bancárias de terceiros;
2. Fraude mediante Invasão de computadores, sejam eles de uso pessoal, empresarial ou mesmo uma rede de computadores;
3. Fraude Mediante Extorsão cibernética e ransomware;
4. Fraude Crimes do tipo phishing, onde a vítima é enganada de modo a compartilhar suas senhas, números de cartão de crédito e outras informações sensíveis;
5. Cryptojacking, situações onde hackers invadem e utilizam os computadores das vítimas para minerar criptomoedas;
6. Violação de direitos autorais;
7. Jogos virtuais de azar ou ilegais em território nacional;
8. Venda de itens ilegais na internet;
9. Incitação, produção ou posse de pornografia infantil;
10. Divulgação de discursos de ódio — com teor homofóbico, xenófobo e racista — e fazer apologia ao nazismo.

Esta Cartilha somente irá discorrer sobre os ciber-crimes que envolvem as práticas mais comuns de golpes financeiros pela internet.

O QUE É FRAUDE?

O termo “Fraude”, remonta sua definição linguística, como qualquer ato ardiloso, enganoso, de má=fé, com intuito de lesar ou ludibriar aguem, ou ainda um ato de falsificar algo. Em linhas Criminais, o nosso código penal definiu o crime genérico de fraude no artigo 171:

> *Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:*
>
> *§ 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.*

O QUE SÃO AS FRAUDES DIGITAIS?

Uma fraude digital é caracterizada por qualquer situação em que dados pessoais ou bancários são usados de forma indevida. Geralmente, essas informações servem para cometer crimes virtuais, que geram prejuízos reais às vítimas, sejam elas empresas ou pessoas físicas.

A quantidade de espécies de crimes virtuais são cada dia mais criativas e crescente em números, sendo algumas mais comuns no nosso dia-a-dia, o que necessita maior orientação à população a fim de evitar o seu acontecimento.

Estima-se que R$ 3,6 bilhões de reais todos os anos, “abastecem” as organizações criminosas somente com crimes cometidos pela internet. Quando relacionamos a quantidade de golpes com seus valores, a média chega a R$ 1.002,00.

O AVANÇO NA ESTRUTURA E A EVOLUÇÃO DAS FACCÕES CRIMINAIS

Todas as organizações buscam evoluir para alcançar seus objetivos, sejam eles comerciais, sejam pessoais, sociais, etc., e porque seria diferente a atuação das organizações criminosas que vêem na internet um solo fértil para arrecadar recursos de maneira fraudulenta. Veja este ponto do editorial da matéria publicada pelo portal Correio Brasiliense em maio deste ano:

> *"Duas das maiores facções criminosas do país, o Primeiro Comando da Capital (PCC) e o Comando Vermelho, entraram com tudo no mundo digital e estão roubando o que podem de brasileiros. Com a vida financeira da população concentrada nos celulares, esses aparelhos se transformaram nos principais alvos de bandidos, diz Rafael Cordeiro, diretor de Vendas da Tempest, uma das maiores empresas de cybersegurança da América Latina, com base em relatos da polícia. Em muitos casos, as vítimas são sequestradas para que todas as informações bancárias sejam repassadas. De posse dos dados, os criminosos abrem contas especialmente em bancos virtuais em nome dos raptados, que são transformados em laranjas deles próprios".*
>
> *"O executivo lembra que, diante dos altos volumes de recursos roubados, o PCC e o Comando Vermelho estão arregimentando um grupo cada vez maior de criminosos. "Eles atuam em todas as frentes. Não só roubando celulares, mas enviando mensagens maliciosas, os phishing. E muita gente cai como peixe na rede", detalha. Os golpes se estendem às empresas, que estão tendo os dados sequestrados, muitas vezes, por falhas nos sistemas de segurança"*
>
> *"Dados mais recentes de crimes cibernéticos mostram que o Brasil aparece no ranking dos cinco países com mais fraudes digitais".*

Com isso percebemos que a evolução das organizações criminosas, atuando no território da Web, vem crescendo, e dificultando a atuação do sistema de segurança pública que deve atuar na prevenção e repressão destes crimes, levantando o questionamento, sobre o que fazer efetivamente para combater e evitar a vitimização por golpes de fraude na internet.

PRINCIPAIS CARACTERÍSTICAS DOS GOLPES CIBERNÉTICOS

Os golpes cibernéticos possuem algumas características marcantes que devem ser levadas em consideração, a fim de que com estas informações sejam evitadas vitimizações destes crimes.

Das Características mais importantes, destacamos a Clandestinidade, que nos termos jurídicos seria a ocultação ilegal que tem por objetivo evitar a publicidade obrigatória de atos, dificultar seu conhecimento por terceiros ou lesar o direito de outrem, pois os criminosos labutam para tentar ocultar informações que possam levar a vítima a perceber que se trata de um golpe;

Outra Característica a se destacar é a localização imprecisa do criminoso, pois este pode estar usando alguma camuflagem que dificulte a localização do dispositivo de onde parte o Golpe;

Também, podemos colocar a manipulação artificiosa do criminoso, que nada mais seria a criação de uma história convincente ao ponto de colocar em erro a vítima que acredita estar tratando de um assunto idôneo, enquanto esta "caindo na rede" criminosa.

O uso de "Laranjas", também é característico dos crimes cibernéticos, por com a facilidade de acesso a bancos de dados fornecidos por Hackers, os dados sensíveis das pessoas e empresas ficam a mercê de criminosos, que em posse de tais informações criam contas bancarias a fim de receberem fraudulentamente recursos advindos de golpes.

A mais lamentável característica, hoje pertinente aos crimes cibernéticos, é a sensação de impunidade, em razão da dificuldade nos processamentos judiciais dos golpes, pois ainda que denunciado pelas vítimas, muitos crimes se tornam verdadeira dor de cabeça para a vítima, que além de perder recursos financeiros ainda se depara com a dificuldade nas investigações que possam levar aos autores e a recuperação dos valores perdidos.

CARACTERÍSTICAS DAS VÍTIMAS DE CIBER-CRIMES

Quando destacamos o ponto de vista dos crimes cibernéticos, levando em consideração as vítimas, percebemos algumas características marcantes que levam as pessoas a serem vitimadas nestes delitos.

Apesar de não ter como definir uma caraterística única das vítimas, podemos definir a que se destaca, que é a **VULNERABILIDADE** e o excesso de **CONFIANÇA**, pois estas duas características são muito exploradas pelos cibercriminosos, que se utilizando da manipulação artificiosa, criam histórias que por muitas vítimas, realmente são tidas como verdadeiras e isso eleva a possibilidade de que acabe por enviar recursos financeiros aos criminosos.

Muitos usuários de tecnológicas conectadas na internet, por serem leigas nestes assuntos, acabam por acatar pedidos de pessoa que de forma clandestina, se passando muitas vezes por parentes, funcionários bancários, delegados, etc., e com abuso da credibilidade adquirida no decorrer do golpe acabam depositando confiança no golpista, acreditando se tratar de algo realmente idôneo, e com isso tornam-se extremamente vulneráveis.

CARACTERÍSTICAS DOS CIBERGOLPISTAS

Quando o enfoque se dá pelo ponto de vista do criminoso, percebemos que a atuação seja ela de modo solitário ou através de ordens advindas de organizações criminosas, das características mais latentes nos golpes cibernéticos destacam-se a **Expertise** desempenhada pelos criminosos, que em posse de diversas informações da vítima passam a criar histórias que até para os mais atentos, o levam a incidir em erro e sofrer prejuízos. Ademais também os criminosos atuam sob o **Princípio da Oportunidade**, ou seja, sempre buscam a forma mais fácil e pratica para o cometimento dos ilícios na internet, e para tanto buscam encontrar vítimas desatentas e vulneráveis a fim de auferirem vantagens de modo fraudulento.

CONTEUDO LEGISLATIVO SOBRE GOLPES CIBERNETICOS

Várias leis contra fraudes digitais já foram criadas no Brasil. As principais modificaram o Código Penal e aplicaram penas mais severas.

1. A primeira delas é a Lei dos Crimes Cibernéticos, de 2012. Também chamada de Lei Carolina Dieckmann, o foco é a tipificação das fraudes. Aquelas com caráter menos grave geram prisão de 3 meses a 1 ano e multa. As mais danosas podem levar à detenção de 6 meses a 2 anos, além de multa.
2. A segunda é o Marco Civil da Internet. Sancionada em 2014, a lei determina quais são os direitos e os deveres dos internautas. Também preserva os dados pessoais e a privacidade dos usuários.
   Assim, fica determinado que os usuários podem solicitar a retirada de um conteúdo ao próprio serviço de hospedagem ou ao site em situações de violações de intimidade. No restante dos casos, é preciso haver a ordem judicial.
3. Em 2021, entrou em vigor a terceira e principal lei de fraudes digitais. A seguir, explicaremos como ela funciona.
   Em maio de 2021, foi sancionada a Lei 14.155. Ela endurece as penas para as pessoas que cometem crimes na internet. Para isso, foi feita uma alteração do Código Penal.

A partir de agora, a pena será de até **8 anos de prisão**. Além disso, ela poderá ser agravada se:

- A vítima for uma pessoa vulnerável ou idosa;
- O crime for praticado com uso de servidor mantido fora do brasil. Ainda haverá a aplicação de multas. Entre os crimes tipificados por essa lei estão:
    a. Invasão de dispositivo;
    b. Furto qualificado;
    c. Estelionato;
    d. Indução ao erro no repasse de informações do usuário via redes sociais, mensagem, contatos telefônicos ou e-mail fraudulento.

Dos crimes cibernéticos que serão punidos com mais rigor, os principais são:

1. Clonagem do WhatsApp e de conta digital;
2. Golpe do falso funcionário de banco;
3. Crimes de phishing (roubo de dados por meio de mensagens e links falsos);
4. Golpe da falsa central telefônica.

FUI VITIMA DE GOLPE, E AGORA?

Caso você seja vítima de um crime na internet, é importante conhecer a lei de fraudes digitais e tomar as providências cabíveis. Nesse caso:

- Colete o máximo de evidências sobre os fatos, como prints de telas, conversas salvas em aplicativos de mensagens, e-mails, etc.;
- Você também pode registrar estes elementos através de empresas que fornecem esse serviço online. Essa etapa é dispensável, mas serve como reforço à alegação de crime cibernético;
- Registre uma **Ata Notorial**. (opcional), mas com certeza vale a pena. Este procedimento é realizado em cartório. O objetivo desta Ata é declarar a validade dos documentos e dos fatos digitais. Para que possam ser usados como prova em uma ação judicial;
- Registre um Boletim de Ocorrência (BO). Leve consigo neste ato todas as evidências à Polícia Civil para esse procedimento. Desse modo, é possível iniciar as investigações nas delegacias especializadas, onde houver.

Agora você já tem uma base do que fazer caso seja uma vítima de crimes cibernéticos. Mais do que isso, passou a entender o que a lei de fraudes digitais diz para cada caso.

Golpe do boleto falso

Esse vem sendo o tipo mais comum de fraude no Brasil. Normalmente, os criminosos elaboram um boleto falso contendo todos os dados da vítima, onde se passam por uma empresa de cobrança real. Eles enviam o boleto via WhatsApp solicitando pagamento. A conta pode ser um financiamento, contas de serviços como telefone, ou pagamentos de compras de produtos.

Como prevenir?
Confira atentamente os dados do boleto e desconfie de mensagens de cobrança advindas de outra pessoa diversa daquela a qual é credor, LIGUE para o credor e tire a dúvida sobre o motivo da data ter mudado, o porquê de nova emissão de boleto, ou seja, a qualquer sinal de mudança de rotina, desconfie e não emita pagamentos sem confirmar a idoneidade.

Golpes via SMS

O SMS é um dos golpes favoritos dos criminosos. Nas mensagens, eles pedem que a vítima atualize cadastros de bancos, enviando links que direcionam para páginas falsas. O objetivo final desse golpe é conseguir os dados pessoais para acessar os canais oficiais. Esses golpistas estão se especializando cada vez mais e contratando sistemas de disparos de mensagens em massa, no qual conseguem atingir um número maior de vítimas. O SMS é semelhante com os recebidos de instituições financeiras, já que ele aparece com o número pequeno no identificador.

Como prevenir?
Não pratique a troca de informações recebidas em seu dispositivo de forma indiscriminada, atente-se para o conteúdo dos links que chegam ao seu dispositivo. Deixe para atualizar dados de preferência presencialmente ou por canais oficias das instituições. Nunca forneça dados sensíveis como senhas, códigos de ativação, entre outros.

Golpe do perfil falso

Nesse golpe, os criminosos usam contas com perfis falsos nas redes sociais. Ele se divide em duas situações: golpistas se passando por contas de lojas, onde vendem os produtos que não são entregues. Nesse caso, a vítima fica no prejuízo e não recebe as compras; quando se passam por pessoas e simulam relacionamentos virtuais, conhecido como Catfish. Eles encontram um alvo e começam a ganhar confiança da vítima. Após estreitarem relações, começam a relatar problemas e dificuldades financeiras, pedindo dinheiro para cobrir despesas. Na maioria das vezes, as mulheres são as grandes vítimas desse tipo de golpe.

Desconfie de relacionamentos e amizades repentinas que solicitam envio de recursos financeiros. Há golpes, onde o criminoso, diz possuir muito dinheiro e que pretende retornar ao Brasil, e para isso precisa que o dinheiro passe pela Alfandega nos aeroportos. Ocorre que, outro golpista se passa por agente aeroportuário e diz ter realizado a apreensão do dinheiro, geralmente dólares, e que algumas taxas de desembaraço precisam ser pagas para liberar o dinheiro. A vítima pensando estar se tornando milionária, deposita dinheiro para que restante seja liberado.

Golpe do investimento

Se tratando de golpes, os criminosos não perdem tempo. Devido ao crescimento de investidores no Brasil, esse tipo de golpe vem aumentando e se especializando. O fraudador promete retorno de investimentos em determinada criptomoeda. E claro, esse investimento não existe. Portanto é muito importante as pessoas estarem atentas para as propostas, o mundo dos investidores é muito volátil e não existem garantias de retornos, então quando alguém oferece uma proposta de que é só aplicar determinado recurso e o retorno será 2x, 10x, 100x mais, tenha em mente que possa se tratar de algum golpe. O investidor sabe que sempre há risco de perda, e nunca uma promessa indiscriminada de ganhos sempre.

Golpe do emprego

No golpe do emprego, o fraudador cria páginas falsas anunciando empregos, mas solicita que a vítima realize um cadastro e que pague um valor para acessar às oportunidades. Com isso, além deles terem acesso aos dados pessoais das vítimas, ainda tiram dinheiro com falsas promessas de trabalho.

Fique atento a páginas de internet que ofertam benefícios além do que seria razoável.

Golpe do suporte técnico

É possível que 70% dos brasileiros já tenham sofrido essa tentativa de golpe, de acordo com a Microsoft. Os criminosos criam pop-ups (aquelas janelas que abrem na tela), alertando que seu computador ou celular está com vírus e precisa ser protegido. Quando a vítima clica no link, abre um falso site de antivírus, e assim, a pessoa paga por um produto que não irá proteger seu celular ou computador.

Golpe do WhatsApp

Com certeza você conhece alguém ou já ouviu falar no golpe do WhatsApp. Os bandidos clonam seu WhatsApp, e mandam mensagens para seus contatos, como familiares ou amigos e solicitam um Pix com urgência, alegando que seu limite diário acabou. Muitas pessoas acabam caindo no golpe e fazem a transferência sem desconfiar. Muitas vezes, os golpistas encontram as fotos em perfis de redes sociais. Por isso, é necessário confirmar sempre as informações em duas etapas, com os códigos de segurança.

Golpes de comércio eletrônico

Exploram a relação de confiança do usuário nos negócios on-line. A vítima pode ser atraída por uma oferta imperdível e não receber a mercadoria comprada ou o pagamento por um produto vendido, além de passar dados seus ao golpista. Algumas dicas para prevenção para esse tipo de golpe:

- Desconfie se o valor do produto está muito abaixo do de outros fornecedores confiáveis;
- Pesquise na internet sobre o site antes de efetuar a compra para ver a opinião de outros clientes;
- Acesse sites especializados para verificar se há reclamações referentes à empresa;
- Fique atento a propagandas recebidas por spam ou redes sociais;
- Utilize sistemas confiáveis de pagamentos para impedir que seus dados pessoais e financeiros sejam enviados ao golpista;
- Em caso de venda, confirme que recebeu o pagamento diretamente na sua conta bancária ou pelo site do sistema de pagamentos (não confie apenas em e-mails ou comprovantes de depósito, pois podem ser falsos);
- Acesse todos os sites, tanto de pagamentos quando de vendas, diretamente do navegador, e não por links recebidos em mensagens;
- Mesmo que o vendedor lhe envie o código de rastreamento fornecido pelos Correios, saiba que isso não basta para comprovar o envio e liberar o pagamento.

Notificações falsas das redes sociais

Um alerta aparece na tela do computador informando sobre notificações das redes sociais, geralmente sobre novos amigos, suas atividades, comentários, curtidas, usuários inserem seus dados de usuário e senha em uma página de login falsa, achando que estão acessando o site oficial da rede social.

Outra variante comum dessa prática são mensagens de mídias sociais que alegam a detecção de atividades suspeitas na sua conta, ou que uma nova ferramenta foi adicionada, a qual necessita de consentimento, sem o qual o usuário seria bloqueado. Seja qual for o caso, a mensagem possui um botão que direciona para um site malicioso que infecta o computador de usuários para roubar dados do sistema.

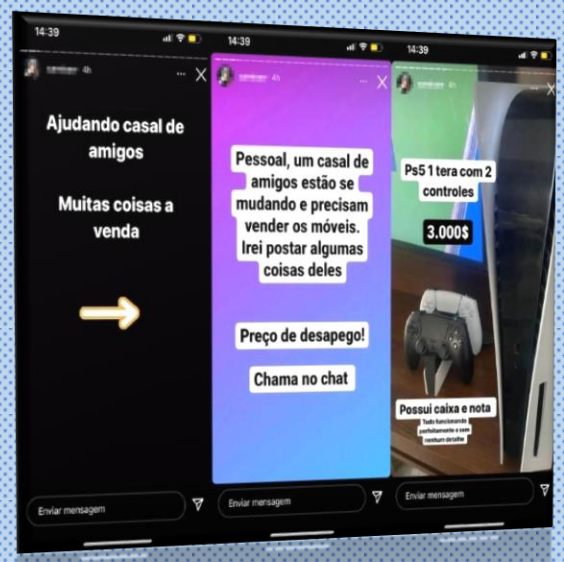
Pacote de dados gratuito

Promessa de pacote com 7 GB / 15GB de internet gratuita para estimular os brasileiros a ficarem em casa diante da pandemia. O benefício era enganosamente atribuído à Agência Nacional das Telecomunicações (Anatel), que divulgou um alerta sobre a fraude. Ao clicarem no link suspeito, as vítimas eram direcionadas a um site que pedia informações sobre a linha telefônica do usuário. Muita atenção a estes tipos de ofertas advindas de supostas operadoras de telefonia.

Agências bancárias / Novo gerente

Ocorre através do envio de mensagens SMS em nome de instituições financeiras alegando o fechamento de agências bancárias, solicitando que a vítima abra um link e preencha um cadastro com informações pessoais. O objetivo é captar informações pessoais dos consumidores. Um outro golpe também aplicado em nome dos bancos é sobre o “novo gerente da conta”. O cliente recebe uma mensagem supostamente do banco, informando que houve uma alteração no gerente da conta. O consumidor recebe um contato do possível novo gerente e o golpista começa a solicitar informações pessoais, alegando que tem novos investimentos e aplicações para indicar ao cliente.

Golpe de venda de mercadorias através de redes sociais



Após conseguir roubar o acesso de plataformas como Instagram, facebook, ou WhatsApp, os criminosos passam a divulgar fotos de produtos a venda, geralmente se tratam de eletrônicos, moveis, entre outros, com preços bem abaixo do valor médio. Também, os criminosos, se passando pelo dono da rede social, alegam estar se mudando para o exterior e precisam se desfazer dos moveis e eletrônicos, passando a vender a “preço de banana”, muitas vezes até doando, cobrando somente o preço de um suposto frete.

Neste caso, cabe ao dono da rede social, divulgar aos amigos que foi vítima de hacker e que não está vendendo nada, por outro lado, cabe a quem acessa as propostas divulgadas, tomar cuidados para não “cair na rede” do criminoso. Procure ligar para a pessoa que está vendendo os produtos, desconfie dos valores muito baixos. Também, procure tomar providencias de segurança ao acesso nas redes sociais.

Golpe do novo número

Diferentemente de quando alguém tem o WhatsApp clonado, situação em que golpistas invadem a conta de uma pessoa de maneira remota, o golpe do novo número é mais simples, mas igualmente perigoso.

Nele, alguém adiciona a sua foto como avatar do aplicativo de mensagens e passa a abordar os seus contatos como se fosse você, alegando que aquele é o seu novo número. Depois, contam alguma história para convencer seus contatos a emprestar dinheiro.

Como se proteger?

- Não compartilhe as suas senhas com outras pessoas e nem forneça esse tipo de informação via mensagem;
- Evite compartilhar a foto do seu WhatsApp em redes sociais. Os criminosos se aproveitam de correntes que viralizam e roubam fotos compartilhadas em perfis abertos;

- Verifique as configurações de privacidade das suas redes sociais e restrinja, mesmo que parcialmente, o acesso às suas informações para quem não for seu amigo ou seguidor;
- Nunca transfira dinheiro para alguém sem antes conferir se está tudo certo. Tente ligar ou fazer uma chamada de vídeo antes de realizar a transação;
- Desconfie de números desconhecidos entrando em contato, mesmo que a foto utilizada seja a de alguém que você conhece. Uma alternativa é tentar entrar em contato ou ligar para o suposto número antigo para checar se aquela mensagem é verdadeira;
- Se você notar algum problema com o seu aplicativo de mensagens e perder o acesso à conta, pode ser que ela tenha sido invadida. Entre em contato com o suporte do app e avise seus conhecidos imediatamente (por uma rede social, por exemplo).

Golpe do Pix

O Pix é pop, e os golpistas logo se aproveitaram dessa popularidade para envolver vítimas em suas armadilhas.

Alguns dos golpes mais comuns envolvendo o Pix neste ano foram os seguintes:

Bug do Pix em dobro

Nas redes sociais, criminosos compartilham vídeos e mensagens dizendo que é possível transferir via Pix e ganhar dinheiro em dobro na conta. De acordo com eles, isso aconteceria devido a uma falha de instituições financeiras e do próprio sistema Pix.

A história que os golpistas contam é que, para funcionar, as pessoas precisam transferir dinheiro para chaves específicas – e, em seguida, compartilham supostos números que funcionam.

Quem transfere o dinheiro para as tais chaves acaba, na realidade, mandando dinheiro direto para os criminosos.

Viu alguma mensagem parecida com essa nas redes sociais? Corre que é cilada.

Desconto na fatura com pagamento via Pix

Recebeu alguma mensagem dizendo que a conta do seu cartão ou do celular pode ficar mais barata se pagar com Pix? Desconfie.

Um dos esquemas funciona assim: criminosos enviam um SMS para a vítima afirmando que operadoras de cartão de crédito se uniram em uma campanha para oferecer desconto caso a fatura seja paga com Pix.

Para isso, a pessoa só precisa acessar um site indicado pelos golpistas e informar dados como bandeira do cartão e os quatro últimos dígitos, CPF e o valor total da fatura. Depois, a página indica uma chave Pix que deve ser usada para o pagamento da fatura com desconto.

Assim que a vítima confirma a transferência, não tem mais volta. Os golpistas transferem o dinheiro no momento em que ele cai na conta e a pessoa termina no prejuízo.

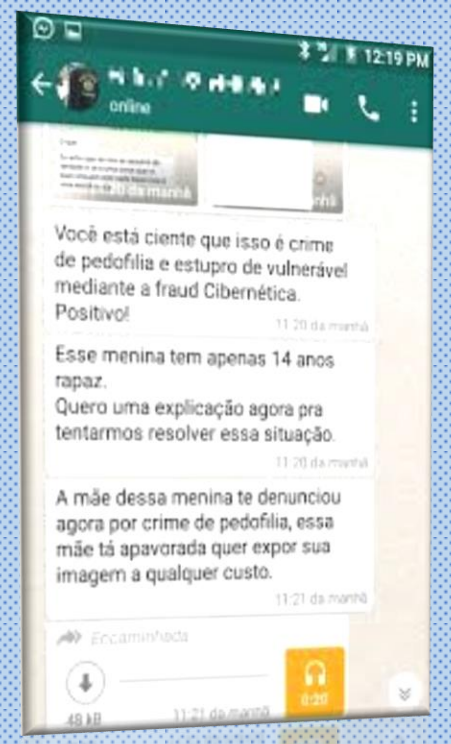
Como se proteger?

- Nunca clique em links que chegam por mensagens – a não ser que você tenha absoluta certeza de que é seguro. Na dúvida, não clique;

- Desconfie de mensagens que prometem dinheiro fácil. Em caso de problemas ou dúvidas, entre sempre em contato com a sua instituição financeira.

Vale lembrar que o Pix é seguro e conta com diversas camadas de proteção. Na realidade, o problema são os criminosos que aproveitam as facilidades desse meio para fazer mais vítimas.

Golpe da novinha



Também conhecido como 'golpe da falsa delegacia'. “Uma pessoa usa uma conta falsa e se faz passar por uma bela mulher. Ela aciona as vítimas pelas redes sociais, como Instagram e Facebook, e estabelece um relacionamento virtual que rapidamente evolui para a troca de fotos íntimas. Quem começa enviando os nudes é o criminoso e quando a vítima envia imagens íntimas que permitem identificá-la, o estelionatário entra em ação”

Nesse momento, a suposta mulher bloqueia a vítima e um falsário entra em contato, se identificando ou como pai da menina ou delegado de polícia. O golpista informa que a moça é menor de idade e pede dinheiro para que a vítima não seja exposta à família, ao empregador, à polícia e à imprensa. “Quando o golpista se apresenta como delegado, envia um vídeo com um trecho da suposta denúncia da mãe da moça. Todo o cenário é montado de forma a levar a vítima crer que se trata de uma delegacia de polícia, tem banner, uniforme e até carteiras funcionais falsificadas. Em alguns casos, enviam documentos falsificados com o timbre da corporação e certidões de nascimento falsas. Assustados, muitos homens não percebem os indícios de fraude e costumam pagar as quantias exigidas para não serem expostos”

Leia mais em: https://www.diariodolitoral.com.br/policia/ja-caiu-no-golpe-da-novinha-conheca-a-nova-modalidade-de-cibercrime/149115/

Golpe do Carro Quebrado

Você já ouviu falar do golpe do carro quebrado? Nesse tipo de crime, os autores fingem ser familiares da vítima e pedem dinheiro para o conserto do suposto carro. A persuasão é a principal arma dos criminosos, que conseguem enganar as vítimas facilmente.

O golpista liga aleatoriamente para as vítimas, geralmente no período noturno.

Independentemente de quem atende o telefone, o golpista logo fala: “oi tio (a), ou oi primo (a), sabe quem está falando?"

Caso a vítima diga um nome, achando ser algum sobrinho ou outro parente distante, já deu ao golpista o que ele queria.

Muitas vezes a vítima fala que não se recorda e então o golpista usa do artifício “nossa, não lembra mais de mim!”, dialogando com a vítima até que seja possível extrair dela um nome de um parente que mora distante.

Com isso, ele forja uma história de que estaria viajando ou chegando próximo à cidade onde a vítima reside, e relata que sofreu algum acidente ou que o carro quebrou. Então o criminoso solicita que a vítima faça uma transferência em dinheiro para determinada conta bancária do mecânico, do guincho ou da borracharia onde o veículo está sendo consertado. Ele promete devolver o dinheiro no dia seguinte quando chegar à cidade da vítima.

Como prevenir?

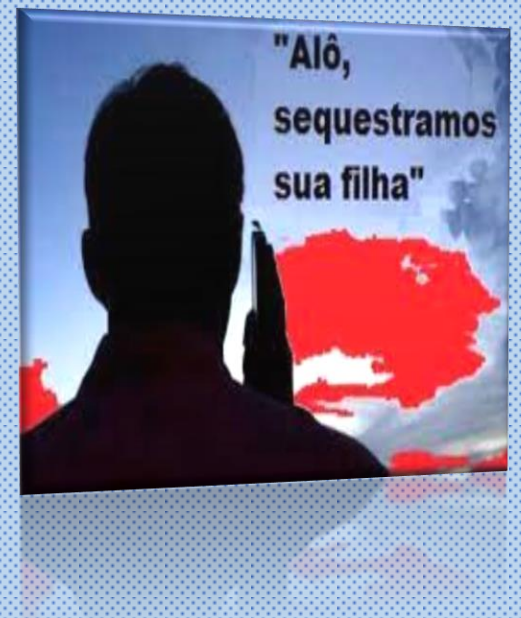
Não faça transferências ou entregue dinheiro para terceiros;
Desligue o telefone e faça contato com o familiar que você achava estar falando.

Golpe do Falso Sequestro

O telefone toca. O número não consta em sua agenda telefônica ou a chamada vem sem identificação. O horário de maior incidência varia entre 10h00 e 16h00. O golpe é simples, funciona por tentativa e erro e vem causando prejuízos financeiros significativos as vítimas, porém seu maior impacto é psicológico, pois durante a sua aplicação a pessoa é atingida por altas descargas de adrenalina e em alguns casos o medo ou pânico se alastra de forma rápida e permanente mesmo após o fim do sinistro.

O criminoso escolhe números aleatórios e começa a busca pela vítima ideal. Pouco importa quantas ligações serão efetuadas ele tem tempo e paciência. Nas primeiras falas pelo tom de voz o roteiro é escolhido. Caso perceba uma voz de uma pessoa madura irá falar rapidamente e com voz pouco clara “mãe, mãe fui sequestrada, fui sequestrada…” ou “pai, pai fui sequestrado, não liga para polícia faz o que mandarem”.

Objetivando, não permitir que a vítima consiga processar as informações com clareza e/ou localizar o seu parente (suposto sequestrado) a ligação não é interrompida ou vai sendo feita em intervalos curtos de um a dois minutos.



Quem recebe a ligação suspeita, precisa manter a calma. Escutar muito e falar quase nada, ser monossilábico. Utilizar um nome fictício para seu parente e observar se o golpista passa a repetir esse nome como se estivesse com alguém em seu poder. Mesmo que ele saiba o nome de algum parente e acerte de primeira, tal fato não significa que ele esteja com a pessoa. Utilizar nomes comuns é uma prática estratégica neste tipo de “negócio”, por um motivo bem simples, todos nós conhecemos algum; João, José, Antônio, Maria ou Ana e o criminoso sabe disso.

Quando receber esse tipo de ligação, a prudência recomenda não fazer nenhuma promessa, não combinar nenhum pagamento.

RESUMO

DICAS PRÁTICAS DE PREVENÇÃO

- Não seja ganancioso, os criminosos usam a engenharia mental para ludibriar suas vítimas ofertando muito dinheiro, muito lucro em troca de pouco dinheiro!
- Nunca deposite dinheiro, sob promessa de receber vantagens;
- Nunca perca de vista seus cartões bancários, caso aconteça o extravio ou perca, providencie o cancelamento e modifique suas senhas de segurança;
- Jamais revele suas senhas pessoais, ou as deixe guardadas em locais de fácil acesso;
- Caso perca seus documentos pessoais, providencie o registro disso junto à polícia;
- Não deixe espaços em branco nos documentos em que assinar, especialmente Cheques; e jamais os deixe assinados com valores em branco;
- Crie a rotina de verificar suas movimentações financeiras, e caso algum valor seja debitado ou creditado de sua conta, procure a instituição para realizar a contestação daquele valor;
- Não forneça seus dados pessoais por telefone, peça que o representante da empresa diga os dados para que você confirme, jamais o contrário;
- Não deposite confiança em estranhos que cheguem em sua casa ou lhe aborde na rua, ou ainda por telefone ou redes sociais;
- Não acesse links na internet sem ter conhecimento de sua procedência;
- Fique atento ao fato de que golpistas geralmente oferecem vantagens no intuito de atrais as vítimas, a procuram agir com pressa no acesso aos valores. Fique Atento a isso";
- Sempre que alguém se passar por familiar ou amigo em apuros, alegando necessitar de recursos financeiros naquele momento, procure tomar as seguintes providencias de confirmação:

    1. Fale um nome aleatório que não seja seu familiar, (é você Pedro?) Como se estivesse reconhecendo o familiar, com isso a tendência do golpista é

confirmar, (sim, sou eu primo!); e isso basta para perceber se tratar de golpe;

- Quando alguém entrar em contato dizendo ter trocado de número, procure ligar no número antigo e confirmar a veracidade, ou até mesmo, perguntar a outros familiares e amigos sobre esta mudança repentina, que em se tratando de golpes, tem uma característica marcante: sempre a troca de número precede a solicitação de dinheiro para ser transferida ou depositada em conta diversa da vinculada aquela pessoa;
- Tome cuidados ao acessar links ou sites, verifique se são os verdadeiros, principalmente sites de empresas lojistas;
- Quando for comprar produtos em sites, procure averiguar se o preço não esta muito abaixo da pratica de mercado, preços extremamente baixos podem ser um sinal de fraude;
- Quando for vender algo pela internet, não envie o produto antes de tomar providencias quanto ao efetivo pagamento, se não foi feito por agendamento e, portanto, passível de ser cancelado;

Idosos: com certeza você tem algum amigo, colega ou familiar idoso, muitos deles possuem pouco conhecimento sobre as ferramentas da internet, então procure orientá-los sobre os riscos da internet;

Caso seja vitimado por um golpe, procure tomar as seguintes providencias:

Verificar junto a instituição financeira o bloqueio ou estorno do valor depositado;

Vá até uma delegacia, especializada de preferência, levando consigo o máximo de provas e informações que possam auxiliar o delegado na investigação do caso;

Procure contatar o máximo de amigos e familiares alertando-os sobre a sua situação: Clonaram meu celular! Não estou vendendo nada! Etc.;

GOLPES, NÃO CAIA NESSA!!!