SEGURANÇA VIRTUAL

TJDFT

Tribunal de Justiça do Distrito Federal e dos Territórios
Gabinete de Segurança Institucional
Assessoria de Segurança Institucional

Polícia Civil do Distrito Federal
Departamento de Polícia Especializada
Delegacia Especial de Repressão aos Crimes Cibernéticos

Sumário

ENGENHARIA SOCIAL

Engenharia social é a habilidade de conseguir acesso a informações confidenciais pessoais ou de áreas importantes de uma instituição, mediante habilidades de persuasão. Não é necessário utilizar equipamento sofisticado para realizar essa atividade, bastando aproveitar-se do pouco conhecimento tecnológico da vítima ou de sua necessidade de exposição social, obtendo dados de pessoas desavisadas, por meio não só da tecnologia, mas da conversa fácil e da confiança. A busca de informações pode ocorrer nos locais mais simples, como mesas de trabalho e lixeiras, e pela atenção às conversas alheias em locais sociais.

COMO SE PROTEGER?

- Oriente familiares, pessoas próximas e auxiliares da família sobre informações que são solicitadas na rua ou por telefone.

- Não clique em links desconhecidos em SMS, e-mails ou publicações em redes sociais.

- Não clique em banner de propagandas.

PHISHING

Esse tipo de golpe tem o objetivo de “pescar” informações e dados pessoais importantes, por meio de mensagens falsas. Com isso, os criminosos podem conseguir nomes de usuários e senhas de um site qualquer, como também podem obter dados de contas bancárias e cartões de crédito.

As vítimas recebem link ou arquivo malicioso por e-mail, mensagem de texto (SMS) ou serviço de mensagem instantânea, como WhatsApp, Telegram e Facebook Messenger, que são criados para parecer emitidos por instituições conhecidas, como bancos, operadoras de telefonia, órgãos do Governo e administradoras de cartão de crédito. No ato de abrir o link ou arquivo, o celular ou computador é infectado por conteúdos fraudulentos que buscam dados pessoais e bancários.

Atualmente, são mais comumente propagadas as seguintes modalidades de phishing:

A) PHARMING: consiste no direcionamento da navegação do usuário para sites falsos;

B) SMISHINGS: são os phishings por SMS, enviados massivamente por meio de empresas especializadas em distribuição de mensagens em larga escala;

C) VISHING: é o phishing de chamada pela tecnologia VoIP (voz sobre IP), utilizado por criminosos para extrair dados bancários ou informações pessoais da vítima. São aplicadas técnicas de falseamento do remetente da chamada, possibilitando ao autor da chamada se passar por atendente bancário, de empresa comercial ou funcionário público;

D) “CHAT-IN-THE-MIDDLE”: envolve a adição de uma janela de suporte de bate-papo ao vivo falsa, na qual a pessoa é estimulada a inserir seus nomes de usuário e senhas.

DICAS DE SEGURANÇA:

- Lembre-se: phishing é um ataque oportunista. Não clique em links desconhecidos em mensagens de SMS, e-mails, WhatsApp ou publicações em redes sociais.

BAITING

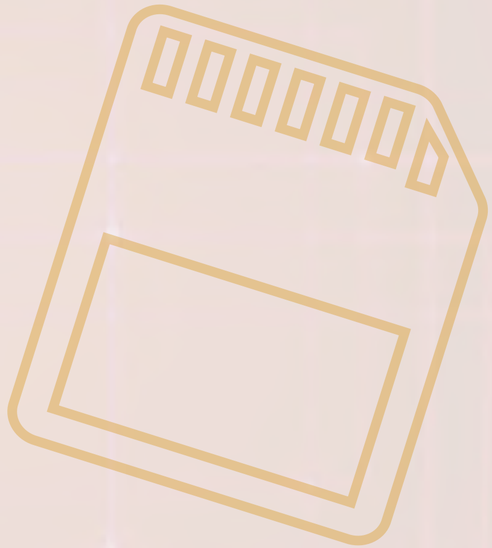
Nesse modelo de golpe, o criminoso “esquece” um pen drive em lugar de muita circulação, contando com a curiosidade do usuário para atraí-lo. Quando a vítima conecta o dispositivo no computador, é instalado um software malicioso sem que ela perceba.

CLONAGEM POR SIM SWAP

A técnica consiste em transferir a linha do chip de um usuário para um chip em branco. Esta modalidade pressupõe a participação de funcionários de empresas de telefonia ou de pessoas por estas autorizadas a realizar a migração de conta para outro usuário. Trata-se de operação ilegal, mas que vem se tornando corriqueira nos últimos anos. Esta situação é bastante delicada, pois as mensagens SMS dirigidas àquela conta passa a ter como destinatário o próprio criminoso. Desse modo, todos os aplicativos que possuem fator de segurança configurado para confirmação via códigos ou tokens encaminhados via SMS, tornam-se extremamente vulneráveis, como no caso de aplicativos bancários e o aplicativo Whatsapp. A conta deste aplicativo de mensageria facilmente é tomada pelo criminoso. Diferentemente dos demais casos, o usuário percebe que está completamente impedido de usar qualquer serviço da operadora, inclusive chamadas telefônicas.

COMO EVITAR:

- Inclua como fator de autenticação o cadastro de uma conta de e-mail válida e protegida por senha considerada forte. Para incluir esse dado na confirmação em duas etapas no WhatsApp, abra: **CONFIGURAÇÕES > CONTA > CONFIRMAÇÃO EM DUAS ETAPAS > ATIVAR**. Após definir a senha de 6 (seis) dígitos numéricos, **incluir a conta de e-mail**. Jamais enviar para outra pessoa a senha desta conta cadastrada.



WHATSAPP

Clonagem do aplicativo

Os golpistas têm diversos meios de conseguir o número de telefone da vítima. Contudo, o mais usual é que seja obtido de anúncios em plataformas de sites de compras ou anúncios públicos em redes sociais (que abrangem não só os contatos da vítima). O golpista identifica que o usuário original do aplicativo fez um anúncio em algum tipo de site ou serviço da internet no qual o número de telefone é exibido para fins de transação comercial.

A vítima recebe SMS do qual consta um código de 6 dígitos. O golpista se passa por funcionário da plataforma de anúncio e solicita o código alegando que isso é necessário para ativar o anúncio. O código, entretanto, foi enviado pela própria empresa WhatsApp ao usuário original do aplicativo, atendendo comando realizado pelo criminoso, a partir do momento em que deu início ao processo de transferência do WhatsApp, sem possuir a capacidade de receber a mensagem de SMS contendo o respectivo código. Este código é uma verificação do WhatsApp, ou seja, o golpista digitou o número de celular da vítima no celular dele para ativar o WhatsApp. É por esse motivo que ele solicita o código, afirmando que isso seria necessário para habilitar o anúncio, induzindo a vítima a fornecê-lo. De posse desse código, o golpista desvia o WhatsApp da vítima para o aplicativo instalado no celular dele, e a vítima perde o acesso ao aplicativo. Após isso, o criminoso inicia conversas com amigos da vítima, fazendo-se passar por ela, alegando estar sem dinheiro, com algum problema na conta bancária ou com cartão de crédito bloqueado, e solicita valores emprestados, comprometendo-se a pagar no dia seguinte. Os amigos da vítima, acreditando tratar-se da pessoa, acabam transferindo o dinheiro para a conta bancária informada, que, normalmente, é de algum “laranja”. Assim que a transferência é efetuada, eles também se tornam vítimas do golpe.

COMO SE PROTEGER?

- É de suma importância habilitar a “confirmação em duas etapas” do WhatsApp. Para ativar a confirmação em duas etapas no WhatsApp, abra: **CONFIGURAÇÕES > CONTA > CONFIRMAÇÃO EM DUAS ETAPAS > ATIVAR**. Você definirá senha de 6 dígitos numéricos. Jamais enviar para outra pessoa o código de 6 números que chegar por SMS.

CAÍ NO Ggolpe. O QUE FAZER?

- Proceda ao registro de ocorrência na Polícia Civil.
- No caso de clonagem do aplicativo, envie e-mail para **support@whatsapp.com** solicitando a desativação temporária de sua conta no aplicativo, explicando o ocorrido, bem como informando o seu número de WhatsApp. Posteriormente, deve- se iniciar a conta com o novo código de verificação.
- Clique no número de telefone que enviou a mensagem e, no campo “dados do contato”, clique em denunciar.
- Se o golpista, após capturar seu WhatsApp, tiver ativado a “confirmação em duas etapas” como forma de evitar a recuperação do aplicativo pelo usuário original, os seguintes procedimentos deverão ser adotados: desinstale e instale o WhatsApp em seu aparelho, digitando os códigos de instalação de forma errada por várias vezes. Repita tal procedimento até bloquear a conta, condição que permanecerá pelo prazo de 7 dias. Após esse período, o usuário receberá um novo SMS com o novo código de ativação.

Clonagem de fotos do perfil

Os criminosos vinculam a fotografia da vítima, normalmente retirada do próprio WhatsApp ou das redes sociais, a um número telefônico. O objetivo é se passar pelo usuário original do aplicativo para pedir empréstimos aos seus conhecidos e familiares ou, também, para obter informações íntimas ou confidenciais.

DICAS DE SEGURANÇA:

- Desconfie de conversas com pessoas cujos números de telefone não estejam salvos em sua agenda. Caso você receba mensagem de algum contato solicitando empréstimo de dinheiro ou depósito de algum valor em determinada conta, confirme com a pessoa a veracidade dessa solicitação. E, caso seja verdade, antes de qualquer confirmação de depósito, verifique os dados do destinatário (nome, CPF e agência bancária).

COMO EVITAR:

- Faça a configuração da foto do perfil para definir por quem ela pode ser vista. Abra o WhatsApp e toque em **Menu (os três pontinhos no canto superior da tela);** a seguir, toque em **Configurações; clique em Conta, Privacidade** e, por fim, em **Foto do perfil**; toque na opção para permitir quem verá sua foto de perfil, se todos os usuários, se apenas os seus contatos (sugerido), ou se ninguém.

Apresentação do status: limitar quem pode ver

Para selecionar quem pode ver o seu status no WhatsApp, clique em **STATUS**, toque nos três pontinhos no canto superior direito e, em seguida, selecione **“Privacidade do status”**. Você terá três opções. A opção padrão é **“Meus contatos”**, ou seja, todas as pessoas cujos números de telefone estejam salvos em sua agenda. Altere para **“Compartilhar somente com...”** e selecione as pessoas que poderão ver suas publicações no status.

WhatsApp Web

É possível verificar se a sua conta está logada em algum computador. Na opção de **“Ajustes”** do aplicativo, vá para a opção **“WhatsApp Web/Desktop”** e verifique quais aparelhos estão com sessões ativas. Se observar alguma atividade estranha, clique em **“Sair de todas as sessões”**.

DICAS DE SEGURANÇA:

- Desconfie de conversas com pessoas cujos números de telefone não estejam salvos em sua agenda. Caso você receba mensagem de algum contato seu solicitando empréstimo de dinheiro ou depósito de algum valor em uma determinada conta, confirme com a pessoa a veracidade dessa solicitação. E, caso seja verdade, antes de qualquer confirmação de depósito, verifique os dados do destinatário (nome, CPF, agência bancária).
- Configure a verificação em duas etapas.
- Proteja seu e-mail vinculado à conta.
- Verifique com frequência as sessões ativas no aplicativo web.
- Nunca forneça códigos solicitados por SMS.
- Não clique em links desconhecidos.

FACEBOOK

É uma das maiores fontes de informação utilizadas pela engenharia social. Por motivos diversos, são publicadas informações valiosas sobre comportamentos, hábitos, estados de espírito e momentos de vida que podem ser utilizados de forma escusa por pessoas mal-intencionadas. É a privacidade exposta ao mundo virtual. Por isso, deve-se ter muito cuidado com o que é postado.

DICAS DE SEGURANÇA:

- Configure a verificação em duas etapas.
- Controle o conteúdo daquilo que publica.
- Não torne públicas informações de natureza pessoal, como parentescos, RG, CPF, número de telefone.
- Evite fotos e vídeos pessoais e com familiares que informem que, naquele instante, estão fora de casa, que possam identificar residência ou locais de trabalho ou, ainda, que identifiquem onde você ou familiares estudam ou trabalham (uniforme).
- Verifique sempre as sessões ativas do seu aplicativo.
- Desabilite a permissão de aplicativos de terceiros.
- Tenha atenção quanto a jogos e páginas pelo Facebook e cuidado com cadastros e acesso a informações.
- Verifique quais aplicativos e sites utilizam os dados do Facebook para acesso. Exclua os que não são necessários. Para verificar, acesse **CONFIGURAÇÕES > APLICATIVOS E SITES > ATIVOS**.

INSTAGRAM

Como o Facebook, o Instagram tem potencial de expor o usuário ao mundo virtual. Da mesma forma, tem-se tornado grande fonte de dados para a engenharia social, o que enseja as mesmas preocupações e cuidados com a proteção dos dados pessoais.

O golpe mais comum é a clonagem de perfil do usuário. Com capturas de tela das fotos postadas, os criminosos passam-se pela vítima, criam uma conta com nome de usuário parecido e dizem ter sofrido um “ataque hacker” no perfil original. Assim, solicitam novo contato para seguir amigos e familiares da vítima. Aproveitando-se da boa vontade deles, passam a enviar mensagens diretas, pedindo depósitos em dinheiro em conta bancária ou de outro tipo de instituição financeira, como, por exemplo, o PayPal, alegando ter perdido o acesso às contas em redes sociais e ao aplicativo do banco.

Outra forma de ação dos golpistas consiste em utilizar as imagens publicadas no Instagram para criar contas supostamente originais, que são usadas com o intuito de atrair potenciais compradores para os materiais postados em páginas fraudulentas ou de conteúdo pornográfico.

DICAS DE SEGURANÇA:

- Configure a verificação em duas etapas.

- Por padrão, qualquer pessoa pode ver seu perfil e publicações no Instagram. Você pode tornar sua conta privada para que apenas os seguidores aprovados consigam ver o que compartilha. Caso sua conta esteja configurada como privada, somente os seguidores aprovados verão suas fotos ou vídeos. Para configurar, vá a **CONFIGURAÇÕES > PRIVACIDADE > PRIVACIDADE DA CONTA > CONTA PRIVADA**.

- Não mostre o status da atividade, que informa quando o usuário esteve on-line.

- Oculte story de pessoas que te seguem e que você não deseja que vejam suas publicações.

- Não permita compartilhamento de story.

TIVE MEU APLICATIVO CLONADO. O QUE FAZER?

O golpe acontece geralmente quando o usuário possui muitos seguidores, e o golpista, usando a engenharia social, apropria-se da conta da vítima e passa a pedir resgate por ela.

Caso um usuário tenha perdido seu acesso ao Instagram, deverá, primeiramente, tentar reavê-lo via Facebook ou SMS. Além disso, é possível acessar a conta de e-mail vinculada ao aplicativo e localizar a mensagem que informa a modificação. Desfaça, caso possível, a modificação de senha.

DICAS DE SEGURANÇA:

- Configure a verificação em duas etapas.
- Use senha distinta para acessar o Instagram e o e-mail vinculado.
- Em caso de invasão criminosa, registre boletim de ocorrência na Polícia Civil.

VERIFICAÇÃO EM DUAS ETAPAS

A verificação em duas etapas ou autenticação de dois fatores é uma técnica de proteção utilizada por diversos sites e aplicações da web. A autenticação de senhas em duas etapas pode até não ser a solução definitiva para a segurança de contas, mas reduz o risco de que contas on-line, redes sociais e serviços bancários sejam atacados por hackers. Funciona, basicamente, como uma etapa a mais nos processos de autenticação de login e senha, que devem ser realizados pelo usuário. Quando necessária a verificação, o aplicativo solicitará a senha de 6 dígitos numéricos criada pelo usuário.

Aplicativos e sites têm características distintas para ativar a verificação em duas etapas:

WHATSAPP

Para ativar a confirmação em duas etapas no WhatsApp, abra: **CONFIGURAÇÕES > CONTA > CONFIRMAÇÃO EM DUAS ETAPAS > ATIVAR**. Você definirá senha de 6 dígitos numéricos. Jamais enviar para outra pessoa o código de 6 números que chegar por SMS.

GOOGLE

No painel de navegação, selecione Segurança. Em **“COMO FAZER LOGIN NO GOOGLE”**, selecione **“VERIFICAÇÃO EM DUAS ETAPAS”**. Siga as instruções dadas pelo site do aplicativo.

FACEBOOK

Acesse **CONFIGURAÇÕES E PRIVACIDADE > CONFIGURAÇÕES > SEGURANÇA E LOGIN > AUTENTICAÇÃO DE DOIS FATORES > USAR AUTENTICAÇÃO DE DOIS FATORES**.

INSTAGRAM

Acesse **CONFIGURAÇÕES > SEGURANÇA > SEGURANÇA DE LOGIN > AUTENTICAÇÃO DE DOIS FATORES > USAR AUTENTICAÇÃO DE DOIS FATORES**. O aplicativo solicitará o código de segurança de confirmação e você poderá confirmar por SMS ou por aplicativo de autenticação.

Você pode usar aplicativos autenticadores para a verificação em duas etapas. Os aplicativos oficiais gratuitos da Microsoft ou da Google estão disponíveis em versões para Android e iOS. O autenticador é uma ferramenta muito simples, com a função de gerar códigos para a validação em dois passos.

PIX

PIX é um novo meio de pagamento instantâneo, criado pelo Banco Central para ser uma nova opção, ao lado de TED, DOC e cartões, para que pessoas e empresas possam fazer transferências de valores, realizar ou receber pagamentos durante 24 horas por dia, inclusive em fins de semana e feriados.

Apesar de o funcionamento do PIX ter iníciado em 16 de novembro de 2020, vários golpes começaram a ser praticados bem antes, principalmente na forma de phishing. O objetivo é coletar dados bancários e pessoais, como senhas bancárias e números de CPF e celular. Os ataques de phishing imitam campanhas legítimas de bancos e fintechs (empresas de tecnologia focadas no mercado financeiro, com serviços exclusivamente digitais), em que são enviados links ou e-mails fraudulentos para que o usuário acesse página falsa e cadastre seus dados.

DICAS DE SEGURANÇA:

- Não clique em links desconhecidos.
- Nunca forneça códigos solicitados por SMS.
- Use os canais oficiais do seu banco ou agente financeiro para saber mais sobre o PIX. Somente cadastre-se pelos meios indicados por eles.
- De forma geral, empresas nunca pedem que os usuários forneçam suas senhas via e-mail, ou seja, bancos, instituições financeiras e operadoras de cartão não vão pedir esse dado. Desconfie de pedidos de dados sigilosos por e-mail.
- Não instale programas nem baixe arquivos em anexos enviados por lojas ou estabelecimentos.
- Na dúvida, contate seu gerente bancário.

FALSO BOLETO

Em tempos de pandemia, em razão do isolamento, muitas pessoas fazem compras pela internet, redes sociais e até mesmo pelo WhatsApp. Muitas vezes, a vítima não tem acesso seguro aos sites visitados, seja pelo computador, seja pelo celular. Diversas são as formas de manipular a vítima nesse momento. Pode ser por uma falsa página de loja ou por falso contato pelo WhatsApp para venda direta. Na conclusão da compra, é emitido o boleto bancário para pagamento. O boleto falso possui cabeçalho e imagens aparentemente da loja ou empresa com que a vítima estava negociando. O golpe pode ser realizado tanto com a manipulação do código de barras do documento quanto com a criação de páginas falsas que oferecem o download da “fatura”. Com o pagamento do boleto, o valor pago vai para a conta bancária do golpista ou de um “laranja”.

DICAS DE SEGURANÇA:

- Mantenha o antivírus e o sistema operacional atualizados.
- Evite abrir links de terceiros e anexos de e-mails de fontes desconhecidas.
- Verifique sempre os dados do destinatário do boleto emitido. Antes de confirmar a transação ou o pagamento, verifique se os dados do beneficiário conferem com os dados da loja/empresa, como logomarca e número do banco.
- Desconfie ao observar erros gramaticais.
- Caso queira emitir segunda via de boleto, procure o site oficial do credor e verifique os dados do boleto emitido.

FALSO SITE

É comum abrir o navegador e, por equívoco, digitar incorretamente o nome do domínio que se pretenda acessar. Aproveitando-se dessa corriqueira situação, os criminosos, para enganar os usuários, criam site fraudulento, praticamente idêntico ao site verdadeiro, de venda de mercadoria (eletrônicos, eletrodomésticos, etc.). Esse golpe costuma ter maior incidência em datas comemorativas e promocionais, como, por exemplo, na black friday. O golpista usa endereços de empresas famosas, alterando só o final do endereço.

DICAS DE SEGURANÇA:

- Observe com cuidado todo o endereço eletrônico.

- Existem algumas precauções que você pode tomar para garantir a segurança da sua navegação. Se você acessar um site e desconfiar dele, verifique se há um ícone de cadeado em algum lugar. Para ser confiável, o site deve ter o cadeado. Não digite seus dados em sites que não possuam esse ícone. Outro local para verificar a existência do cadeado é ao lado da URL da página. Ao clicar nele, será exibido o certificado de segurança.

- No site www.whois.net, você pode verificar as informações de registro do site.

- Pesquise a reputação da empresa eletrônica em que pretenda efetuar a compra.

- Desconfie de objetos que estejam à venda por preço muito abaixo daquele praticado no mercado.

OUTROS GOLPES

Golpes em sites de compras on-line (OLX)

A vítima faz um anúncio em site de compras on-line, expondo seu número de telefone para contato. De posse do número de telefone, o golpista, por mensagem ou ligação telefônica, engana a vítima, dizendo que há necessidade de atualização da conta/cadastro no site ou de verificação do anúncio. Para validar a “atualização” ou a “confirmação” do anúncio, o golpista solicita que a vítima lhe informe os 6 dígitos numéricos que ela receberá por SMS, em seu celular. Todavia, esses números são, na verdade, o código de validação da conta do WhatsApp.

DICAS DE SEGURANÇA:

- Habilite a verificação em duas etapas no WhatsApp.
- Não repasse códigos recebidos via SMS, sem antes verificar a veracidade da solicitação feita pelo interlocutor.

Falso sequestro

O golpista geralmente é um presidiário que telefona de maneira aleatória para diversos números. Quando a vítima atende, o bandido grita ao fundo, como se fosse uma pessoa “sequestrada”. A vítima, desesperada, fala o nome de um filho, sobrinho, alguém próximo. Com isso, o bandido consegue a informação que queria para fazer a vítima acreditar que se trata de sequestro de verdade. No momento de tensão, a vítima não percebe que foi ela mesma quem forneceu o nome do suposto sequestrado e, frequentemente, em razão do nervosismo, não percebe a diferença na voz. Nesse momento, o golpista exige que a vítima não desligue o telefone e permaneça na linha até que alguém faça a transferência de determinado valor para a conta de algum “laranja”.

DICAS DE SEGURANÇA:

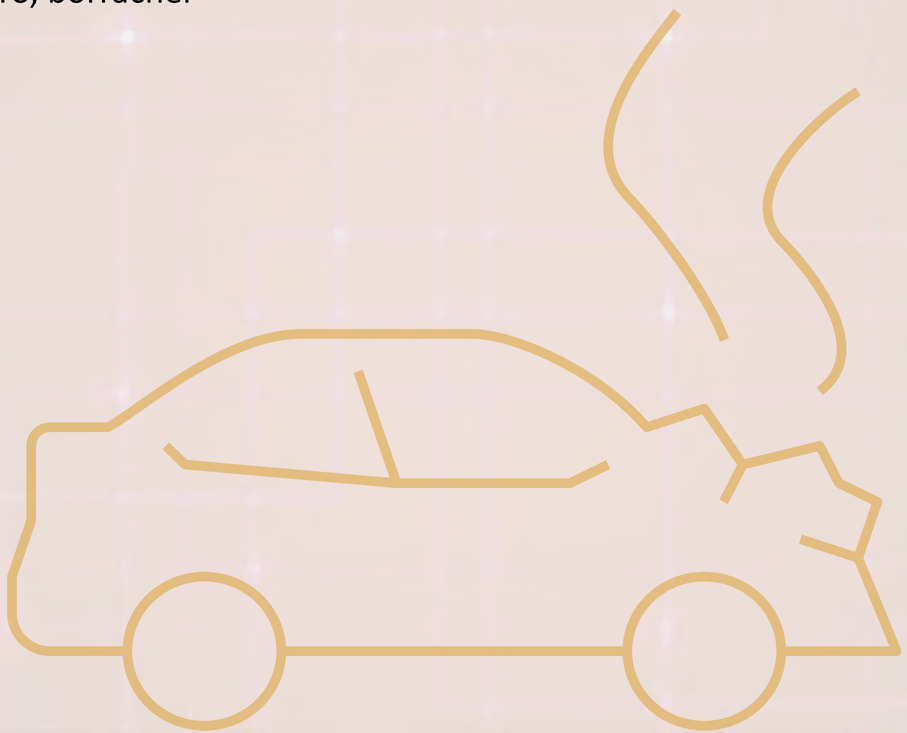
- Encerre a ligação e faça contato com o suposto familiar que teria sido sequestrado. Caso tenha receio de encerrá-la, acreditando ser verdadeiro o sequestro, peça a alguém próximo (familiar ou vizinho) que contate a suposta vítima do sequestro para constatar a veracidade da informação.

Parente com carro quebrado

O golpista telefona aleatoriamente para as vítimas. Dependendo de quem atenda, homem ou mulher, ele costuma dizer: “oi, tio/tia, sabe quem está falando?” Caso a vítima diga um nome, achando ser algum sobrinho ou parente distante, o golpista conseguiu o que queria. Algumas vezes, a vítima fala que não se recorda, e o golpista diz: “nossa, não se lembra mais de mim?”. A vítima, constrangida, acaba continuando o diálogo e se sujeitando ao que o golpista fala. Com isso, ele afirma que seu carro quebrou e que precisa de ajuda, solicitando que a vítima faça transferência para determinada conta (mecânico, lanterneiro, borracheiro etc., para pagar o conserto do carro).

DICAS DE SEGURANÇA:

- Não faça transferências nem forneça dinheiro para terceiros.
- Encerre a ligação e contate o familiar com quem você achava estar falando. Caso a pessoa esteja realmente em apuros, você ainda poderá ajudá-la.



Falsa clonagem de cartão bancário

O golpista faz contato com a vítima, apresenta-se como funcionário da administradora do cartão de crédito, alega que houve uma compra duvidosa no cartão da vítima e solicita que ela confirme ou não a compra. Como a vítima não reconhece a compra, o golpista solicita a ela que ligue para o número de telefone que consta no verso do cartão para pedir o cancelamento da compra e o bloqueio do cartão. Nesse momento, a vítima não percebe que o golpista continua na ligação. Após a vítima "discar" para o número de telefone instruído, o golpista coloca uma gravação como se fosse do banco. Acreditando que está falando com uma pessoa da operadora do cartão, a vítima fornece seus dados pessoais (nome completo, RG, CPF, data de nascimento e endereço para onde é encaminhada a fatura) e do cartão de crédito (número do cartão, nome como consta do cartão, data de vencimento da fatura, data de validade do cartão, código verificador — aquele de 3 dígitos contido no verso do cartão — e senha). Depois de obter essas informações, o suposto atendente da administradora do cartão informa que enviará uma pessoa (funcionário do banco ou motoboy que trabalhe para o banco) para recolher o cartão clonado. De posse do cartão e dos dados pessoais da vítima, os golpistas fazem compras em diversas lojas físicas ou sites.

DICAS DE SEGURANÇA:

- Caso você receba ligação afirmando tratar-se de loja, instituição financeira ou administradora de cartão de crédito e que seu cartão foi clonado, ou requerendo que você confirme alguma compra que não tenha feito, procure sua agência bancária ou faça contato com o seu gerente de conta. Jamais entregue o seu cartão a alguém. Nenhuma instituição financeira ou administradora de cartão de crédito envia pessoas a residência de cliente para recolher cartão clonado.

Intermediador de vendas

O golpista obtém o número de telefone da vítima em sites de compras e diz ter interesse no objeto anunciado. Com o início da negociação, ele pede que o anúncio seja retirado da plataforma. Com as informações do bem anunciado, o golpista cria novo anúncio com as mesmas fotos postadas pelo próprio vendedor no anúncio original, mas com valor bem abaixo do preço praticado, o que desperta interesse de outros possíveis compradores. Para a pessoa interessada em vender o bem, o golpista diz que comprará o bem anunciado e que, com a aquisição, pagará dívida que possui com algum cliente, sócio, amigo ou irmão e, portanto, pede sigilo no momento de apresentar o objeto para um outro interessado (suposto credor da vítima), prometendo lucro financeiro nessa negociação sigilosa. A pessoa interessada em comprar o bem também é orientada a manter segredo, com a promessa de que ganhará desconto no preço. Com todo esse enredo, o golpista fornece uma ou algumas contas bancárias diversas da conta da vítima que está vendendo o bem, normalmente de “laranjas”. Quando a negociação é de venda de veículo, as vítimas — vendedor e comprador — ainda são orientadas a ir a um cartório para preencher o documento de transferência do veículo e o recibo da venda, para dar mais veracidade ao negócio.

Quando as vítimas percebem o golpe, o dinheiro da negociação foi depositado na conta de um desconhecido, que, logo em seguida, saca todo o montante, o que impede a recuperação do dinheiro.

DICAS DE SEGURANÇA:

- Mantenha o diálogo aberto entre vendedor e comprador. Não aceite realizar negócios em segredo a pedido de terceiros. Sempre procure ver o objeto anunciado pessoalmente, em local público, movimentado e durante o dia. Converse e reforce a negociação pessoalmente. Na hora de efetuar o pagamento, verifique nome, CPF e número da conta do beneficiário.

Troca de cartão por falso funcionário de agência bancária

A vítima, tendo sido observada por um dos golpistas ao inserir dados do cartão em caixa eletrônico, é abordada ao sair da agência bancária por outra pessoa que se apresenta como funcionário do banco — normalmente bem vestido e com crachá do banco. O criminoso alega que houve algum problema na transação efetuada ou na máquina e solicita que a vítima retorne ao caixa eletrônico para verificarem a transação. Nesse momento, ele "auxilia" a vítima e rapidamente efetua a troca do cartão. Às vezes, para a troca, o golpista solicita apenas que a vítima permita que ele verifique o cartão.

DICAS DE SEGURANÇA:

- Nunca entregue seu cartão a terceiros. Caso precise de ajuda na agência bancária, procure sempre o funcionário da instituição financeira e, mesmo assim, não entregue seu cartão. Escute as orientações e faça o procedimento. Caso não tenha muito conhecimento para operar a máquina, peça para que alguém de sua confiança o acompanhe até o banco.

DICAS FINAIS

Não forneça seus dados pessoais (nome completo, CPF, RG, endereço, número da conta bancária e senha) para estranhos, em ligações telefônicas, mensagens SMS ou WhatsApp.

Evite redes Wi-Fi públicas.

Desconfie sempre de ofertas de produtos com preços abaixo dos praticados em mercado.

Não converse com estranhos na rua, tampouco aceite propostas que pareçam ser muito boas e que lhe trariam alguma espécie de “vantagem”.

Saiba que estelionatários falam bem, estão normalmente bem vestidos e facilmente persuadem as vítimas. Tome cuidado para não se tornar mais uma vítima deles.

Exclua informações de natureza pessoal (RG, CPF, conta bancária, telefone, etc.) de seus aplicativos. Você não sabe se, eventualmente, perderá ou terá seu smartphone furtado.

Não publique em redes sociais imagens, vídeos ou fotos que revelem fatos e dados sobre você e sua família, que revelem atividades profissionais, locais de moradia, trabalho e estudo.

Não troque fotos nem vídeos íntimos pela internet/rede social.

Em caso de dúvida, peça ajuda a alguém de sua confiança.

Pesquise sites e telefones na internet em https://www.reclameaqui.com.br/.

Desative Wi-Fi e Bluetooth quando não estiver utilizando.

Instale antivírus no smartphone e mantenha-o atualizado.

Utilize senhas fortes e distintas para seus aplicativos e outros serviços. A senha é pessoal.

Não escaneie QRCode com o celular em sites desconhecidos.

- Habilite a verificação em duas etapas de seus aplicativos.
- Evite utilizar o WhatsApp Web em conexões públicas ou pouco confiáveis.
- Verifique, com frequência, as sessões ativas do smartphone.
- Mantenha a versão dos seus aplicativos atualizada.
- Desabilite a permissão de aplicativos de terceiros.
- Desabilite a geolocalização.
- Caso você tenha sido vítima de algum dos golpes mencionados nesta cartilha, entre em contato:
  Central de Operações de Segurança (COS) do TJDFT
  Telefone e Whatsapp (61) 3103-7190;

  Polícia Civil do Distrito Federal
  Disque-denúncia: 197, opção 0; WhatsApp da Polícia Civil (61) 98626-1197; E- mail: denuncia197@pcdf.df.gov.br; Internet: www.pcdf.df.gov.br ou procure a Delegacia de Polícia mais próxima.
- Em tempos de pandemia, você pode registrar a ocorrência on-line: https://delegaciaeletronica.pcdf.df.gov.br/.

TJDFT