GUIA TELOS DE SEGURANÇA CONTRA GOLPES E FRAUDES FINANCEIROS CIBERNÉTICOS

TELOS
Fundação Embratel de Seguridade Social

O **GUIA TELOS DE SEGURANÇA CONTRA GOLPES E FRAUDES FINANCEIROS CIBERNÉTICOS** objetiva orientar a identificação de algumas ações aplicadas por meio da internet que causam perdas financeiras e como evitá-los. Principais pontos de atenção para evitar armadilhas dos golpistas também fazem parte do conteúdo, lembrando que o tema não é conclusivo, tendo em vista que novas modalidades surgem a cada dia de acordo com a criatividade dos cibercriminosos.

A era digital aliada ao avanço da facilidade de conexão via internet com o uso da grande variedade de dispositivos eletrônicos tem impulsionado o aumento da ocorrência de ciberataques que prejudicam pessoas e empresas. São golpes e fraudes financeiros por meio da tecnologia da informação em que, infelizmente, muitos são vítimas, e só vão perceber a ocorrência após o evento.

Os golpistas conhecidos como cybercriminosos exploram fragilidades dos usuários, procuram enganar e persuadir suas vítimas a fornecerem informações sensíveis ou a realizarem alguma ação que possa comprometer a segurança deles e de toda uma organização.

Toda a estrutura de fraude financeira lida com uma tendência que, infelizmente, grande parte das pessoas tem: a vontade de obter ganhos fáceis e rápidos. Os golpes podem ser mais ou menos sofisticados, mas sempre seguem essa premissa do investimento supervantajoso. Parece um clichê, uma obviedade, mas as pesquisas da Comissão de Valores Mobiliários - CVM mostram que essa prática segue firme, fazendo novas vítimas diariamente. Sendo assim, fuja dos ganhos fáceis.

VAMOS CONHECER OS GOLPES FINANCEIROS MAIS COMUNS E SABER COMO PREVENI-LOS?

1 GOLPE DO ACESSO REMOTO

Um contato de suposto gerente de Banco afirmando que a conta está com problemas e que a solução é baixar um aplicativo para que o técnico consiga analisar e solucionar o caso é a base do golpe que segue pedindo para a pessoa acessar um link e baixar o aplicativo. Feito isso o golpista passa a ter controle total do celular e consegue gerenciar tudo e, é lógico, faz transações financeiras e transferência de valores.

COMO SE PROTEGER

Se receber esse tipo de contato, desconfie na hora. Seu banco não entra em contato solicitando instalação de aplicativos. Assim, nunca baixe aplicativos desconhecidos recebidos por meio de dispositivos eletrônicos.

"Ih, cai no golpe!"

A dica é: *desligue imediatamente o aparelho ou deixe-o desconectado para tentar impedir que os golpistas continuem procurando por senhas ou realizem novas transações.*

2 GOLPE DO PUMP AND DUMP

Remete à Sabedoria Popular: *se a esmola é demais, o santo desconfia.* A ação consiste em inflar (e largar) o preço de uma ação por meio das temidas, mas nem sempre observadas fake news ou pessoas influentes que disseminam rápido a informação recomendando a compra da ação.

As pessoas, sem refletirem sobre a veracidade do fato, começam a comprar aquele papel desesperadamente que faz o valor saltar na bolsa de valores sem nenhum fundamento e de forma forçada.

COMO SE PROTEGER

Recomendações de compra e venda de ação só de profissionais credenciados pela CVM. Sempre verifique a certificação da pessoa para ver se é um profissional credenciado. *Indague!*

3 GOLPE DO WHATSAPP

O aplicativo muito usado para troca de mensagens instantaneamente tem sido alvo de cibercriminosos. Por meio do WhatsApp os ataques estão se aprimorando.

O *golpe com utilização da foto e até áudio de um familiar e amigo por meio de invasão de uma conta com o objetivo de pedir dinheiro está circulando no WhatsApp.* Em muitos casos, o golpista se passa por um conhecido e se vale de conversas anteriores para pedir algum tipo de dinheiro. Caso suspeite, entre em contato por outra rede social com a pessoa que está pedindo dinheiro (ou até mesmo por telefone), para saber se a conta dela não foi fraudada por um golpista antes de qualquer transferência de dinheiro ou até mesmo de interação.

COMO SE PROTEGER

Desconfie de pessoas pedindo dinheiro ou seus dados por aplicativos de mensagem. *Geralmente os golpistas apelam para alguma urgência falsa e pedem depósitos e transferências via Pix para contas de terceiros* ou então para pagar alguma conta.

O ideal é ativar a autenticação de duas etapas do WhatsApp. Para realizar o processo, é preciso abrir o aplicativo, clicar em "Ajustes", depois em "Conta" e em "Confirmação em duas etapas". O aplicativo vai pedir a indicação de uma senha, que deve ser inserida sempre que o aplicativo solicitar. Essa ação protege o WhatsApp de invasões e clonagens.

Outra forma de proteção é não salvar contatos com nomes demarcativos como "amor", "esposa", "mãe", "pai", "vovó".

4 GOLPE DO FALSO BOLETO

Com a facilidade de acesso aos dados pessoais, o emissor do boleto falso pode se utilizar de várias artimanhas fazendo com que a situação seja convincente. O boleto pode chegar como uma falsa correspondência bancária ou de uma loja, ou, ainda, no formato eletrônico, em forma de mensagens de SMS, WhatsApp ou e-mail que direcionam para páginas falsas para download de uma fatura forjada. Os golpistas alteram informações dos boletos, tais como CPF ou CNPJ do emissor, data de vencimento, valor, se passando por beneficiário.

Em geral, os boletos falsos são muito parecidos com os originais. Ao pagar por um boleto adulterado, o valor é direcionado para a conta do fraudador ao invés do verdadeiro credor.

COMO SE PROTEGER

É essencial ficar atento aos dados do beneficiário do boleto. Independentemente da forma como será realizado o pagamento, essas informações são exibidas antes que você complete a transação. Verifique dados como CPF ou CNPJ do emissor, data de vencimento e principalmente o valor para ter certeza que está pagando o documento correto. Veja também se os três primeiros números do código de barras de fato correspondem ao código do banco.

Desconfie de e-mails recebidos com descontos no boleto. A orientação também é não imprimir os boletos. A recomendação é solicitar que o emissor disponibilize o arquivo no formato PDF.

5 GOLPE DO PIX

O cibercriminoso envia um comprovante de Pix para a vítima dizendo que transferiu o valor para a conta dela por engano. O golpista então pede que a pessoa transfira o valor de volta para a conta dele, já que não passa de um engano.

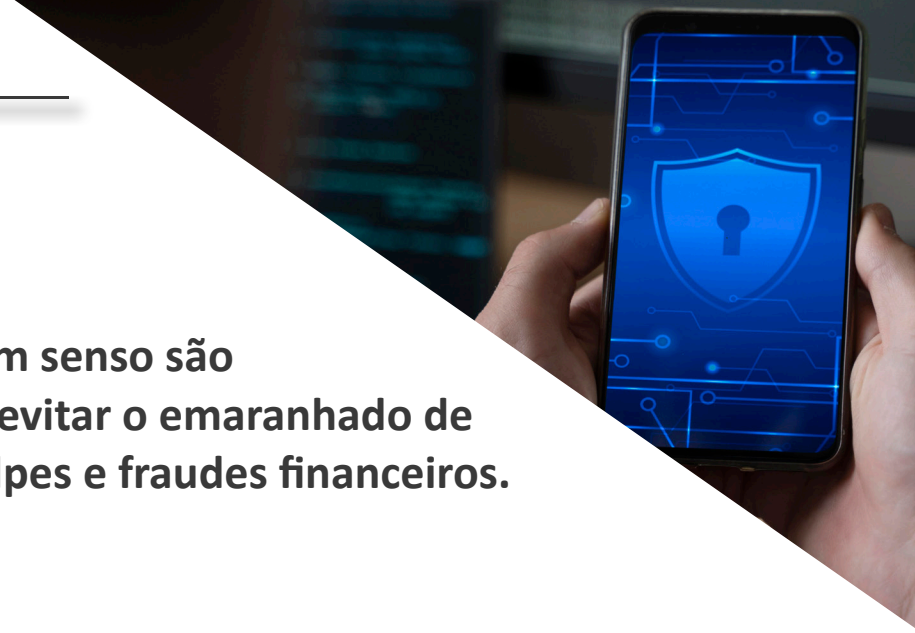
A verdade é que o comprovante do Pix é falso e, se a vítima "devolver" o dinheiro, vai ter caído na armadilha.

Além disso, uma das formas de fazer pagamentos por Pix é via QR Code. Atualmente, é comum vermos QR Code para transferências em lives e apresentações online que arrecadam dinheiro para artistas ou instituições. Os golpistas fazem o download desses vídeos e criam uma nova transmissão com um QR Code falso, divulgam o vídeo e o dinheiro vai direito para a conta do criminoso.

COMO SE PROTEGER

Confira o extrato da sua conta para verificar se realmente entrou algum dinheiro. O Pix é rápido e em apenas alguns segundos a transferência, se for verdadeira, já aparece na sua conta. Quando o Pix for verdadeiro é possível verificar, no extrato, o valor e o botão de devolução. Nunca transfira diretamente para o destinatário e, caso ainda haja dúvidas, verifique diretamente com seu banco.

Ao fazer doações, transferências e pagamentos por Pix, via QR Code, fique atento a origem do código e se desconfie dos valores ou mesmo da origem da solicitação, não complete a operação.



NÃO CAIA NAS ARMADILHAS

A calma, discernimento e bom senso são poderosas ferramentas para evitar o emaranhado de artimanhas utilizadas nos golpes e fraudes financeiros.

DE OLHO NO **PORTUGUÊS**

- ***Verifique se o uso de linguagem*** é adequado à língua portuguesa.
- Atenção a mensagens com ***gírias e abreviações.***

OBSERVE O **REMETENTE DA MENSAGEM**

O ***endereço de e-mail é conhecido***, está escrito corretamente?

O ***número de celular*** é confiável?

Logo apresentada no WhatsApp não é sinônimo de confiança.

Pesquise a reputação e os canais de comunicação da empresa que enviou mensagem.

CUIDADO COM A **EXPOSIÇÃO NAS REDES SOCIAIS**

- ***Configure e ajuste a privacidade de suas redes sociais:*** revise suas configurações de privacidade regularmente para garantir que apenas as pessoas certas vejam suas informações.
- ***Geolocalização:*** conheça e controle quais aplicativos têm acesso à sua localização e habilite-a apenas quando necessário.
- ***Não revele muito sobre você:*** as informações de perfil podem ser bastante úteis para atacantes cibernéticos. Assim, evite compartilhar informações detalhadas sobre você (onde mora, estuda ou trabalha, por exemplo). Também é recomendável ter cuidado ao publicar atualizações de atividades, fotos, vídeos e localização nas redes sociais.

APARELHOS **ELETRÔNICOS PROTEGIDOS**

Ative a biometria: ela reforça a segurança do seu dispositivo.

Confira se o aplicativo é confiável: sempre verifique o nome do aplicativo que você pretende baixar e quem é o desenvolvedor, pois, os aplicativos falsos são muito parecidos com os oficiais. *Confira também informações como:* confiabilidade do desenvolvedor, quantidade de pessoas que instalaram o aplicativo e opinião dos usuários.

Não clique em tudo que receber: esteja alerta a links e anexos que você recebe por e-mail, SMS e aplicativos de mensagem. Caso não conheça o destinatário da mensagem, atenção redobrada. Não abra links, arquivos ou baixe programas ou aplicativos encaminhados a você. Outra dica importante é desconfiar de mensagens que te ofereçam brindes ou prêmios em troca de informações pessoais (nome, CPF, número de cartão ou celular, e-mail, etc).

Não deixe senhas bancárias salvas: evite armazenar informações sensíveis onde ficam facilmente acessíveis.

Fotos de documentos salvas em seu e-mail e dispositivo nem pensar: documentos pessoais são alvos fáceis para os golpistas.

Evite portar celular nas ruas com acesso aos aplicativos bancários. Deixe em casa.

"NEM TUDO QUE RELUZ **É OURO**"

Desconfie de qualquer promessa milagrosa. Promoções muito chamativas, investimentos com lucratividade altíssima e vantagens muito absurdas podem ser um grande indicativo de que algo está errado.

Este Guia é uma iniciativa da TELOS para 11ª Edição da Semana Enef

11ª Semana Nacional de EDUCAÇÃO FINANCEIRA

Fique atento, esses são os dados oficiais da TELOS!

E-mail: relacionamento@telos.org.br
WhatsApp TELOS: (21) 97436-0512
Telefones: (21) 2121-6900 ou 0800 970 6900

Conheça nosso site: www.fundacaotelos.com.br