PROJETO DE LEI Nº155/2024

Institui Campanha Permanente de Combate aos Golpes Virtuais no Município de Santa Bárbara d´Oeste e, dá outras providências. Autoria: Vereador Eliel Miranda

A Câmara Municipal de Santa Bárbara d´Oeste decreta:

Art. 1º - Fica instituída Campanha Permanente de Combate aos Golpes Virtuais no Município de Santa Bárbara d´Oeste.

Art. 2º - São objetos da Campanha:

I - Golpes de comércio eletrônico, compartilhado através de e-mails, mensagens telefônicas, WhatsApp e similares;

II – Pharming, golpe que envolve o redirecionamento da navegação do usuário para sites falsos;

III – Phishing, prática para tentar obter dados pessoais e financeiros de um usuário utilizando técnicas de engenharia social;

IV – Boato (ou hoax) golpe em que a mensagem tem conteúdo falso e alarmante utilizando páginas fakes de empresas importantes ou órgão governamental.

V – Furto de identidade;

VI – Antecipação de recursos;

VII – Golpe do emprego; e

VIII – Golpe de páginas falsas ou clonadas.

Art. 2º - São objetivos da Campanha:

I – Promover a divulgação de conteúdos informativos listando os tipos de golpes virtuais e as maneiras de prevenir esses golpes segundo instruções fornecidas pelos órgãos de segurança;

II – Promover fóruns e canais de debate com a participação de representantes de segurança urbana e sociedade em geral para proporcionar ações de combate e enfrentamento de novas ocorrências;

III – Divulgar canais oficiais para a realização de denúncias formuladas pelas vítimas e aquelas pessoas que identificarem o possível golpe virtual antes de sua ocorrência.

IV- Combater e denunciar sites falsos, mensagens suspeitas recebidas por meio de e-mails, mensagens telefônicas, WhatsApp e toda a atividade suspeita disseminada pela internet que causem riscos ou prejuízos à população de modo geral.

V – Promover movimentos e debates com a participação de órgão de segurança pública urbana para conscientizar a população sobre mecanismos de prevenção e combate a pratica de golpes virtuais.

VI – Auxiliar as vítimas quanto ao procedimento a ser adotado para denúncias e qualquer outra ocorrência;

VII – Acompanhamento quanto a prevenção e controle de novos casos.

Art. 4º - A Campanha deverá ser realizada permanentemente com a participação da população junto aos órgãos oficiais em todos os equipamentos públicos do Município de Santa Bárbara d´Oeste.

§ 1º - A Campanha deverá ser institucional e balizada pelos instrumentos legais e canais oficiais denúncias podendo ser veiculadas através de sites oficiais e cartazes a serem afixados em local de fácil visualização, podendo ser adicionadas outras intervenções que forem necessárias.

§ 2º - Poderão ser desenvolvidas apresentações promovidas por órgãos de segurança para conscientização da população em locais públicos a serem definidos em Lei.

Art. 5º - Esta Lei entra em vigor na data de sua publicação.

Plenário "Dr. Tancredo Neves", 12 de setembro de 2024

ELIEL MIRANDA
Vereador

EXPOSIÇÃO DE MOTIVOS

A presente propositura tem como objetivo principal prevenir golpes virtuais cometidos através de cybercriminosos que usam a tecnologia para aplicar crimes na internet. Suas vítimas podem ser atraídas por promoções veiculadas em sites clones e/ou falsos de lojas de atacado e varejo; podem ser persuadidas através de ligações, gravações e mensagens via SMS, email e WhatsApp de agências bancárias falsas a informarem dados pessoais e financeiros e terem suas contas invadidas por criminosos que através de transferências pix "limpam" o dinheiro das vítimas.

Segundo informações do Tribunal de Justiça do Estado de São Paulo, os cybercriminosos lista outras técnicas comuns de crimes cometidos na internet e dicas de prevenção.

A saber: Furto de identidade: alguém se passa por outra pessoa para obter vantagens ilícitas. A vítima poderá perder dinheiro e temporariamente crédito, ou até ter sua reputação abalada. Pode ser demorado e trabalhoso reverter todos os problemas causados pelo impostor. A melhor forma de impedir que sua identidade seja usada por terceiros é proteger o acesso aos seus dados e às suas contas de usuário.

Antecipação de recursos: um golpista induz a vítima a fornecer informações confidenciais ou a realizar um pagamento adiantado com a promessa de que esta receberá um benefício. Em algum tempo, a vítima percebe que o benefício não existe, que foi vítima de um golpe e que seus dados e/ou dinheiro ficaram com o golpista. Desconfie de situações em que é necessário efetuar um pagamento antecipado para receber um valor maior. Não se empolgue tão rápido com uma possibilidade de ganhar dinheiro, nem sequer responda a esse tipo de oportunidade. Se acreditar que pode ter algum valor a receber, tome a iniciativa de procurar informações oficiais.

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.

Phishing: um golpista tenta obter dados pessoais e financeiros de um usuário utilizando técnicas de engenharia social. A consequência pode ser o vazamento de informações pessoais e financeiras, além de infectar o computador com códigos maliciosos. Fique atento a mensagens recebidas que tentem induzi-lo a fornecer informações, instalar ou executar programas ou clicar em links. Acesse a página da instituição que supostamente enviou a mensagem e procure por informações.

Pharming: golpe que envolve o redirecionamento da navegação do usuário para sites falsos. A consequência será o vazamento de dados pessoais e financeiros, com possível perda financeira. Desconfie se, ao digitar o endereço do site no navegador, você for redirecionado para outro site, o qual tenta realizar alguma ação suspeita, como abrir um arquivo ou instalar um programa. Para se proteger, escolha um provedor de internet confiável, verifique se há erros no nome do endereço do site que você quer acessar e sempre siga as dicas e orientações sobre segurança da informação. Se você está desconfiado de um site, inclusive de um banco, faça login com uma senha errada. Como um site falso não tem como conferir a sua senha, a próxima tela mostrará que é golpe.

Boato (ou hoax): a mensagem tem conteúdo falso e alarmante e geralmente é enviada por uma empresa importante ou órgão governamental, e até mesmo por um conhecido. Pode trazer problemas tanto para aqueles que a recebem e distribuem, como para aqueles que são citados em seu conteúdo, como conter códigos maliciosos, espalhar desinformação pela Internet, comprometer a credibilidade e a reputação de pessoas envolvidas. Com a leitura atenta de uma mensagem desse tipo é possível identificar informações sem sentido e tentativas de golpes, como correntes e pirâmides. Não deixe que sua boa vontade o impeça de verificar a procedência e de conferir a veracidade do conteúdo da mensagem.

Golpe do boleto falso: Normalmente, os criminosos elaboram um boleto falso apresentando os dados da vítima, e se passam por alguma

empresa de cobrança confiável. O WhatsApp ou e-mail envia um boleto. O falso boleto pode ser de conta de telefone, financiamento ou pagamentos de compras de produtos.

Golpe do emprego: Nesse tipo de golpe, o fraudador cria páginas falsas fazendo anúncios de empregos, mas solicita que a vítima realize um cadastro e que pague uma taxa para ter acesso às oportunidades. Com isso, além dos criminosos, terem acesso aos dados pessoais das vítimas, ainda conseguem dinheiro com as falsas oportunidades de trabalho.

Golpe de páginas falsas: Essa prática é comum, e por meio desse golpe, os criminosos conseguem roubar dados pessoais das vítimas, dinheiro ou até mesmo conseguem instalar um malware (um tipo de software malicioso) nos dispositivos, com o intuito de roubar informações da vítima.

Golpe via SMS: O SMS é um dos golpes mais usados pelos criminosos. Nas mensagens via SMS, os criminosos solicitam que a vítima atualize cadastros de bancos, por meio de links que redirecionam para páginas falsas. O objetivo desse golpe é obter dados pessoais para acessar os canais oficiais de Bancos. Esses golpistas estão se especializando cada vez mais e contratando sistemas de disparos de SMS em massa, conseguindo assim alcançar um número maior de vítimas. O SMS é bastante semelhante com as mensagens oficiais recebidas de instituições financeiras, já que ele aparece com o número pequeno no identificador.

Golpe do WhatsApp: Os criminosos perpetram esse golpe ao enviar mensagens que contêm links, os quais direcionam para sites falsos ou instalam aplicativos maliciosos capazes de roubar informações do dispositivo móvel da vítima. Como exemplo, podemos citar o envio de descontos para compra de produtos, ofertas de emprego, isenção de IPVA, entre outras. Outro tipo de golpe cometido pelo WhatsApp é a clonagem de contas, onde os criminosos se apoderam da conta dos usuários, isso ocorre geralmente por meio da solicitação do código de verificação via SMS, e depois se passam pela vítima para requisitar dinheiro dos contatos.

Pelo exposto e com vistas a necessária e urgente intervenção junto aos órgãos pertinentes solicito aos nobres pares a aprovação da presente Lei.

Plenário "Dr. Tancredo Neves", em 12 de setembro de 2024.

ELIEL MIRANDA
Vereador

Assinaturas Digitais

O documento acima foi proposto para assinatura digital na Câmara Municipal de Santa Bárbara d´Oeste. Para verificar as assinaturas, clique no link: http://santabarbara.siscam.com.br/documentos/autenticar?chave=B2GKHVCFBGGKN4S3, ou vá até o site http://santabarbara.siscam.com.br/documentos/autenticar e utilize o código abaixo para verificar se este documento é válido:

Código para verificação: B2GK-HVCF-BGGK-N4S3

ELIEL MIRANDA
Vereador
Assinado em 12/09/2024, às 15:07:08

Câmara Municipal de Santa Bárbara d´Oeste, 12 de setembro de 2024