Classificação: Pública

Segurança da Informação

Cartilha de Segurança Digital

Classificação: Pública

Segurança Digital e Prevenção a Golpes Cibernéticos

Orientações práticas para proteger informações digitais pessoais e corporativas.

Apresentação da Cartilha e Importância da **Segurança Digital**

Importância da Segurança Digital

A segurança digital é essencial para proteger empresas e clientes contra golpes cibernéticos sofisticados e frequentes.

Conteúdo da Cartilha

A cartilha oferece dicas práticas, exemplos de golpes reais e orientações para identificar fraudes comuns.

Responsabilidade Compartilhada

A segurança da informação depende da atenção e atitude responsável de usuários e empresas.

Prevenção e Confiança

Adotar boas práticas digitais fortalece a confiança e ajuda a prevenir riscos financeiros e fraudes.

Antes de iniciarmos: vamos conhecer os golpes cibernéticos mais frequentes.

Phishing
E-mail falso pedindo para “atualizar sua senha” com um link malicioso.
Pode acontecer por e-mail, SMS (smishing) ou até ligação (vishing).

Falsas lojas online
Sites ou perfis em redes sociais vendendo produtos com preços muito abaixo do mercado.
Ex. você paga e nunca recebe o produto.

Golpe do PIX
Golpistas usam urgência ou falsidade para induzir transferências.
Ex. “familiar” pedindo dinheiro com número novo.

Golpe do boleto falso
Muito comum no Brasil. O atacante altera ou envia boletos com código de barras fraudado.
Ex. Você recebe um boleto aparentemente legítimo, mas o dinheiro vai para o golpista.

Engenharia social
Explora o fator humano, manipulando a vítima para fornecer informações ou acesso.
Ex. alguém se passando por suporte de TI pedindo sua senha.

Vazamento e uso de credenciais (Credential stuffing)
Uso de dados vazados para acessar contas.
Ex. você reutiliza senha e tem sua conta invadida.

Clonagem de WhatsApp
O criminoso tenta obter o código de verificação do seu número e assume sua conta.
Ex. Ele pede dinheiro para seus contatos fingindo ser você.

Malware / Ransomware
Software malicioso que infecta seu dispositivo.
Malware: rouba dados.
Ransomware: bloqueia seus arquivos e exige pagamento.

Golpe do “suporte técnico”
Pop-ups ou ligações dizendo que seu computador está infectado.
Objetivo: fazer você instalar algo ou pagar por “suporte”.

Sumário

01 Golpe do Boleto Falso:
Como Funciona e Como se Proteger

Funcionamento do Golpe

Golpistas criam boletos falsos visualmente semelhantes, alterando dados essenciais para desviar pagamentos.

Cuidados para Prevenção

Verifique nome do beneficiário, valor, data e dados bancários antes de pagar qualquer boleto.

Evitar Pagamentos de Fontes Não Oficiais

Evite pagar boletos recebidos apenas como imagens ou PDFs sem confirmação nos sites oficiais.

Ações em Caso de Dúvida

Não realize pagamentos sem confirmar autenticidade pelos canais oficiais da Inpasa para evitar prejuízos.

02 Phishing:
E-mails e Mensagens Falsas

Técnica de Phishing

Phishing envolve mensagens falsas que imitam empresas confiáveis para roubar dados sensíveis ou infectar dispositivos.

Sinais Comuns de Phishing

Erros de gramática, remetentes suspeitos e links encurtados são sinais frequentes de mensagens de phishing.

Medidas Preventivas

Nunca clique em links suspeitos e sempre acesse sites oficiais digitando o endereço no navegador.

Importância da Cautela

Verificar origem e desconfiar de mensagens inesperadas ajuda a prevenir golpes de phishing eficazmente.

03 Golpes:
via WhatsApp e Redes Sociais

Golpes em Redes Sociais

Golpistas usam WhatsApp e redes sociais para enganar com identidades falsas e pedidos urgentes de dinheiro.

Confirmação da Identidade

Sempre confirme a identidade do contato antes de agir em mensagens suspeitas para evitar fraudes.

Proteção de Dados Pessoais

Não compartilhe dados pessoais ou bancários por aplicativos de mensagem ou redes sociais para evitar clonagem.

Uso de Canais Oficiais

Utilize sempre canais formais da Inpasa para confirmações financeiras e contatos oficiais.

04 Cuidados Essenciais no Dia a Dia Digital

Verificação de Autenticidade
Sempre confira a autenticidade de boletos, e-mails e mensagens para evitar golpes e fraudes digitais.

Uso de Sites Oficiais e Atualizações
Acesse apenas sites oficiais e mantenha sistemas e antivírus atualizados para proteger seus dados.

Senhas Fortes e Autenticação
Use senhas fortes e únicas com autenticação em dois fatores para maior segurança digital.

Desconfiança e Atenção
Desconfie de ofertas vantajosas e solicitações urgentes para evitar decisões impulsivas e golpes.

05 O Que Fazer em Caso de Suspeita de Golpe

Interromper Ação Imediatamente

Ao suspeitar de golpe, pare todas as ações, não realize pagamentos nem compartilhe informações pessoais.

Salvar Evidências Importantes

Guarde prints, e-mails, números e links para ajudar na análise e bloqueio de ataques futuros.

Contato com Autoridades

Informe o suposto dono do “boleto” e seu banco rapidamente para receber orientações e tentar bloquear transações suspeitas.

Comunicação e Prevenção Coletiva

Reportar golpe ajuda a proteger outras pessoas e fortalece a segurança contra fraudes.

Se identificar tentativas de golpe utilizando a identidade da Inpasa, comunique prontamente o time de Segurança da Informação por meio do e-mail segurancadainformacao@inpasa.com.br

06 Mensagem Final e Compromisso com a Segurança da Informação

Compromisso Contínuo com Segurança

A segurança da informação é um esforço compartilhado entre a empresa e seus clientes para prevenir fraudes e proteger dados.

Uso de Canais Oficiais

Sempre utilize os canais oficiais para dúvidas, confirmações e solicitações, garantindo maior segurança nas operações financeiras.

Importância da Verificação

Verifique todas as solicitações, especialmente as urgentes, para evitar transtornos e prejuízos financeiros significativos.

Participação Ativa do Usuário

A atenção e a adoção de boas práticas pelos usuários são essenciais para fortalecer a segurança e evitar golpes cibernéticos.

SEGURANÇA DA INFORMAÇÃO

INPASA
MAIS QUE ENERGIA