CARTILHA DE PREVENÇÃO A GOLPES E FRAUDES

"PREVENÇÃO A GOLPES E FRAUDES DIGITAIS"

PÚBLICO

ELABORAÇÃO

Claranet Brasil

APROVAÇÃO

Dengo Chocolates

PÚBLICO

SOBRE ESTA CARTILHA

A Dengo Chocolates respeita e segue as diretrizes da Lei Geral de Proteção de Dados (LGPD).

Nós temos o compromisso permanente em levar ao seu publico conhecimento e informação relevante sobre o tema Prevenção a Golpes e Fraudes Digitais.
Dessa forma, a cartilha traz para orientações para a ampliar a proteção dos dados e informações, além de permitir o bom uso e navegação no mundo digital, destacando ao público sobre seus direitos e deveres com a instituição.

ENCARREGADO DE PROTEÇÃO DE DADOS (DPO)

Encarregado pelo Tratamento de Dados Pessoais: profissional responsável pelo canal de comunicação entre o Controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), a quem compete, entre outras atribuições, aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências de proteção aos dados pessoais dos titulares.

O Sr. Tayan Yudice é o Encarregado pelo Tratamento de Dados Pessoais (“DPO”), exercendo a atuação como canal de comunicação entre o Controlador, Titulares dos Dados Pessoais e a ANPD.
A forma de contato para que os Titulares dos Dados exerçam seus direitos é através do e-mail lgpd@dengo.com

PÚBLICO

OBJETIVOS DA CARTILHA:

01 **Introduzir** o assunto de maneira simples e didática.

02 **Esclarecer** quanto aos fundamentos de Prevenção a Golpes e Fraudes.

03 **Informa**r como evitar cair em golpes ou fraudes.

04 **Fornecer** exemplos adequados à realidade da Dengo Chocotes.

05 **Conscientizar** sobre os colaboradores e público sobre o tema.

PÚBLI

1. Conceitos

ENTENDA O QUE É GOLPE do PHISHING

O phishing é uma forma a qual o golpista tenta roubar informações importantes ou extrair dinheiro ou levá-lo a revelar informações pessoais - tais como números de cartões de crédito, informações bancárias ou palavras-passe - em sites que fingem ser legítimos.

Normalmente, os golpistas no ambiente digital fingem ser de empresas verdadeiras, amigos ou conhecidos numa mensagem de e-mail falsa, que contém acesso para um site falso.

Mesmo que você não saiba o que é **phishing**, já deve ter recebido um e-mail com o título "Atualize seus dados", "Promoção de Produtos" ou "Você deve pagar o Boleto do Banco". Essas mensagens são extremamente comuns e se configuram em um cibercrime conhecido como **PHISHING "Pescar a vítima".**

Ele consiste em tentativas de fraude para obter ilegalmente informações como número da identidade, senhas bancárias, número de cartão de crédito, entre outras, por meio de e-mail com conteúdo duvidoso.

Os cibercriminosos se passam por autoridades ou empresas confiáveis (bancos, lojas, instituições renomadas, Correios e Governo). Para ter sucesso, eles convencem o destinatário de que a mensagem é real, abordando assuntos de interesse das vítimas, como novas modalidades de financiamento bancário e anúncios de

interesse público.

Há uma série de técnicas que os cibercriminosos utilizam para roubar informações, as duas mais comuns são:

- **E-mail/Spam:** consiste em mensagens falsas relacionadas a bancos ou instituições, que levam o destinatário a fornecer seus dados pessoais. O mesmo e-mail é enviado para milhares de pessoas.
- **Malware:** após o usuário clicar em um link disponível no e-mail, o programa malicioso começa a funcionar na máquina coletando informações. Também pode ser anexado em arquivos para download.

Enquanto o **PHISHING** ataca pessoas físicas em massa, o **SPEAR PHISHING** tem empresas como alvo. Esse tipo de e-mail simula uma mensagem enviada por conhecidos departamentos como TI, RH, Comercial ou Financeiro para o colaborador.

Ou o falso e-mail pode utilizar o nome de colegas de trabalho, para tentar tirar vantagem. Ao cair nesse golpe, o profissional coloca todos os dados da empresa em risco. Essas informações em controle de cibercriminosos pode ser muito prejudicial.

ENTENDA O QUE É GOLPE QUISHING OU O PHISHING DE QR CODE

O Quishing, também conhecido como golpe do QR Code, se baseia em estratégias para enganar o usuário para que escaneie um QR Code não verdadeiro e acesse um site fraudulento, baixe um vírus ou inclua informações confidenciais em um formulário.

Muito cuidado ao acessar um código QR “QR Code”, e sempre verifique se você está acessando o site original ou a informação oficial. Tenha muita atenção e cuidado antes de realizar pagamentos.

2. Todos juntos ao combate a golpes e fraudes

O PAPEL DE TODOS NO COMBATE A GOLPE E FRAUDE:

Você possui um papel muito importante no combate a tentativas de golpe e fraude na empresa.

Além de usar recursos tecnológicos para evitar fraude ou golpe, é preciso que todos estejam atentos as modalidades de cibercrime e participem dos treinamentos, pois vão trazer informações importantes e nos preparar para as ações corretas.

Todos nós devemos realizar capacitações orientadas a LGPD, Privacidade e Proteção de Dados, além de treinamentos, conteúdos e materiais de Segurança e Cibersegurança para compreender o conteúdo assimilado e assim evitar a cair em golpes e crimes cibernéticos.

Como instituição ética e comprometida é nosso dever aumentar a conscientização e segurança digital a todos, inclusive a você visitante, cliente e fornecedor.

Em qualquer suspeita ou dúvida, muita atenção, PARA NÃO CAIR NUM GOLPE OU FRAUDE.

3. Evitar o golpe ou fraude

COMO IDENTIFICAR UMA SUSPEITA E NÃO CAIR EM GOLPE OU FRAUDE:

1. **IDENTIFIQUE O QUE PODE SER GOLPE, ANALISANDO O ENDEREÇO DE E-MAIL**

É comum a utilização de nome de remetente falso. A mensagem foi enviada com o nome do banco, mas pode conter um endereço de e-mail sem ligação com a instituição. É preciso, ainda, atenção com endereço de e-mail que possui o nome de alguma corporação, mas apresenta uma grande extensão com muitos números e abreviações.

2. **PRESTE ATENÇÃO EM ERROS ORTOGRÁFICOS**

Se você recebe uma mensagem com erros de ortografia, desconfie. Um e-mail legítimo de grandes empresas raramente contém erros ortográficos e de gramática.

3. **NÃO CLIQUE EM LINKS SEM ANTES VERIFICAR**

Ao passar o mouse em cima do link disponível, você verá a URL com o endereço da página a ser aberta.

Verifique, se for um endereço estranho, não clique.

4. **NÃO ABRA ANEXOS SEM VERIFICAR SE SÃO CONFIÁVEIS**

Esses arquivos possuem malware anexados. Eles podem danificar o computador, roubar suas senhas, além de espiar suas ações, câmera e microfone.

5. NÃO FORNEÇA INFORMAÇÕES PESSOAIS

Bancos, Correios, Empresas e Administradoras de cartão de crédito não pedem dados ou atualizações dos clientes por e-mail, e sim geralmente por sistemas. Em caso de dúvida, entre em contato com os responsáveis pelo telefone ou pelo site oficial da empresa.

6. NÃO CONFIE NAS IMAGENS

Para maior chance de sucesso, os cibercriminosos usam logotipos, cores e slogan das marcas para dar mais veracidade ao e-mail. Por mais que pareça ser uma mensagem verdadeira, desconfie.

Não forneça foto ou biometria, sem entender qual a finalidade de uso e ler a política de privacidade. Este são dados pessoais sensíveis e o uso indevido podem causar graves impactos e dados aos titulares.

Ao entenderem o que é phishing e spear phishing e conhecerem as medidas para combatê-lo, os visitantes, colaboradores e as empresas terão mais condições de protegerem os dados contra esse tipo de golpe.

7. VERIFIQUE O REMETENTE

Em vários casos golpistas ou hackers enviam mensagens ou realizam ligações para aplicar golpe.

Você pode ligar a pessoa que lhe enviou o e-mail ou mensagem para confirmar a veracidade da solicitação, antes de liberar informações, dados ou realizar pagamentos.

Você conhece as pessoas e uma ligação de verificação pode evitar problemas.

Se você não conhecer o remetente, redobre a atenção!!!

PÚBLICO

4. Dicas e Prevenção

COMO EVITAR "GOLPE ou FRAUDE"

- Não responder ou clicar em links em e-mails que peçam informações pessoais, financeiras ou de contas;
- Ao invés de clicar nos links nos e-mails, vá diretamente às páginas digitando o endereço em seu navegador;
- Caso esteja em uma página segura, procurar o "https" no começo do URL e o ícone de um cadeado em seu navegador;
- Manter atualizado o antivírus, navegador de internet e atualizações de segurança de seu computador e execute verificações em seu sistema regularmente;
- Revisar suas contas e login regularmente e verifique atividade não autorizada;
- Utilizar um navegador que possua um filtro de "phishing";
- Suspeite de e-mails que foram enviados em horários após o expediente comercial, afinal você conhece a rotina de seus colegas, fornecedores. Ex: não é comum receber mensagens de madrugada ou feriados;
- Suspeite de e-mail ou ligação que tenham erros de ortografia ou comunicação;
- Ligue para a pessoa que lhe enviou o e-mail ou mensagem para confirmar a veracidade, antes de liberar informações ou realizar pagamentos.**Afinal você conhece as pessoas e uma ligação para a verificação evitará problemas.**
- Verifique se o QR Code físico não foi sobreposto, ou seja, o falso QR Code colado por cima do verdadeiro.
- Valide se o QR Code lhe direcionou a uma página verdadeira.
- Antes de inserir suas credenciais de login, suas informações pessoais ou instalar um malware no dispositivo, pare pense e analise.

- Se o QR Code lhe direcionar para baixar algum arquivo ou aplicativo, acesse a página oficial.

5. Na dúvida ou suspeita de golpe ou fraude

Na dúvida ou suspeita, lembre-se: **Pare, Pense, Analise.**

Comunique seu gestor imediatamente para auxiliar na identificação de uma tentativa de fraude ou golpe.

"NÃO SEJA FISGADO,
NÃO DEIXE O DADO SER ROUBADO OU VAZADO"

PÚBLICA

6. Política de Privacidade Intelectual

Todo o conteúdo descrito neste documento é de autoria da Claranet Brasil para a Dengo Chocolates. É expressamente proibido copiar frases, trechos ou reproduzir material presente neste documento, sem a prévia autorização da empresa, conforme lei 9610/98. Caso haja violação da cartilha aqui mencionada, medidas legais serão aplicadas.

7. Vigência e Controle de Versões

Esta cartilha entra em vigor a partir da data de sua disponibilização aos Destinatários e será periodicamente revisada e atualizada pelo responsável quando houver necessidade ou obrigação legal.

ELABORAÇÃO:	APROVAÇÃO:	ALTERAÇÃO:	DATA:
Claranet Brasil	Dengo Chocolates	Versão inicial	20/06/2025

REVISÃO:	APROVAÇÃO:	ALTERAÇÃO:	DATA:
Claranet Brasil	Dengo Chocolates	Versão inicial	20/06/2025

PUBLIC