

MANUAL DE BOAS PRÁTICAS CONTRA PHISHING

Grupo Magnus – Guia Oficial de Segurança

Elaborado por RS Data Security

1. Introdução

O Grupo Magnus está sujeito a tentativas constantes de engenharia social, principalmente via e-mail, WhatsApp e SMS.

O objetivo deste manual é **capacitar todos os colaboradores** a identificar, evitar e reportar tentativas de phishing, reduzindo riscos como:

- Roubo de senhas corporativas
- Acesso não autorizado a sistemas internos
- Sequestro de dados (ransomware)
- Fraudes financeiras
- Vazamento de informações sensíveis
- Comprometimento da imagem institucional

A segurança começa **individualmente**, mas o impacto é sempre **coletivo**.

2. O que é Phishing?

Phishing é uma técnica onde criminosos tentam:

- se passar por uma instituição confiável (ReclameAQUI, Justiça Federal, bancos etc.)
- induzir o usuário a clicar em um link
- solicitar login/senha
- baixar arquivos infectados

- confirmar informações pessoais ou de empresa

O phishing é hoje responsável por mais de **70% dos incidentes corporativos no Brasil** (dados ANPD, Febraban, IBM).

3. Exemplos Comuns

Os atacantes usam temas que geram URGÊNCIA ou MEDO:

- ReclameAQUI: “Reclamação urgente aguardando sua resposta”
- Justiça Federal / PJe: “Processo judicial pendente”
- RH: “Atualização obrigatória – eSocial”
- Financeiro: “Nota fiscal em divergência”
- Suprimentos: “Confirmação de pedido”
- TI: “Atualização de senha expirada”
- WhatsApp: “Seu código de verificação”
- Entregas: “Falha na entrega do pacote”

Todos esses temas já foram usados em ataques reais no Brasil.

4. Como identificar phishing

✓ 4.1 Verifique o remetente

Nunca confie no nome exibido — verifique o e-mail REAL.

⚠ Exemplos perigosos (parecem legítimos mas não são):

- comunicacaoreclamacoes@reclameaquiatendimento.com.br
- notificacoes@pje-jf3.gov.br
- beneficios@esocialcorp.com

Use a regra:

Se você nunca recebeu e-mails desse endereço antes → Desconfie.

✓ 4.2 Erros de português e formatação

Phishing costuma ter:

- vírgulas fora de lugar
- espaçamento estranho
- falta de acentos
- linguagem “formal demais” ou “robótica”

✓ 4.3 Links suspeitos

Antes de clicar:

1. Passe o mouse por cima do link (**hover**).
2. Veja se o endereço é estranho:
 - ngrok
 - app
 - host
 - aws
 - godaddy

Exemplo:

<https://fc9d625c9acd.ngrok.app> → Nunca é um domínio de instituição oficial.

✓ 4.4 Anexos inesperados

Arquivos perigosos:

- .ZIP
- .HTML (muito usado para phishing)
- .PDF falso que abre login
- .EXE
- .DOC com macros

Regra: se você não esperava o arquivo → Não abra.

✓ 4.5 Solicitação de Senha

Nenhum sistema legítimo solicita senha via:

- link externo
- formulário HTML

- e-mail
- SMS
- WhatsApp

5. Como agir diante de e-mail suspeito

✓ Passo 1 — Não clique

Nada de:

- links
- anexos
- botões
- QR Codes

✓ Passo 2 — Capture informações

Antes de apagar:

- Print da tela
- Copie o e-mail do remetente
- Copie o link suspeito (sem clicar)

✓ Passo 3 — Encaminhe para TI

Encaminhe para:

 ti@magnusimagens.com.br

ou o canal oficial que a empresa determinar.

Assunto:

“Suspeita de Phishing – (descrição curta)”

✓ Passo 4 — Aguarde orientação

Não tente investigar por conta própria.

É papel do time técnico.

6. Boas Práticas Diárias para evitar ser vítima

✔ 6.1 Use MFA (Autenticação multifator)

A senha sozinha **não protege nada**.

✔ 6.2 Atualize seu navegador

Chrome, Edge e Firefox corrigem falhas a cada semana.

✔ 6.3 Nunca reutilize senhas

Senhas repetidas são o maior risco em empresas.

Recomendações:

- Use senhas fortes (12+ caracteres)
- Misture letras, números e símbolos
- Não use informações pessoais

7. Boas práticas específicas para o Grupo Magnus

✔ *Confirmar pedidos apenas pelo sistema oficial Magnus*

Nunca por link enviado por e-mail.

✔ *Chamados internos somente no canal oficial*

Nada de:

- “clique aqui para abrir chamado”
- “sua senha expirou”

✓ **Nenhum documento judicial chega por e-mail**

Justiça Federal **NÃO** envia PDF ou link fora do PJe oficial.

✓ **ReclameAQUI corporativo sempre via login oficial**

Nunca via link externo.

8. Checklist anti-phishing

ITEM	VERIFICAÇÃO	OK?
1	Remetente é conhecido/usuado antes?	<input type="checkbox"/>
2	Domínio é correto (magnusimagens.com.br)?	<input type="checkbox"/>
3	Existe urgência exagerada?	<input type="checkbox"/>
4	O texto tem erros?	<input type="checkbox"/>
5	Link aponta para domínio estranho?	<input type="checkbox"/>
6	Pede senha ou dados?	<input type="checkbox"/>
7	Confere com as práticas internas?	<input type="checkbox"/>

9. Se clicou sem querer

- Desconectar da internet
- Avisar TI
- Trocar senha
- Monitorar acessos

10. Conclusão

Segurança é responsabilidade de todos.

Um único clique errado pode comprometer:

- dados da empresa

- dados dos clientes
- financeira
- reputação
- continuidade das operações

Com atenção e prática, qualquer colaborador se torna capaz de identificar phishing e proteger o Grupo Magnus.