GOLPES DIGITAIS

O que são?
Como são aplicados?
Como prevenir-se?

Por Pedro Pinheiro Guedes

O QUE SÃO GOLPES VIRTUAIS?

- Golpes virtuais são fraudes cometidas pela internet para enganar pessoas e obter informações pessoais, dados financeiros ou dinheiro de forma ilícita, utilizando técnicas como páginas falsas, mensagens fraudulentas e clonagem de contas.
- No Brasil, os golpes virtuais têm crescido muito, tornando-se um dos maiores desafios da segurança digital, com milhares de ataques registrados por minuto e grande prejuízo financeiro para vítimas.

CONCEITOS GERAIS

O ELO MAIS FRACO DA DA SEGURANÇA

- Mesmo com sistemas robustos, o Fator Humano continua sendo a principal brecha.
- Clicar em links suspeitos, usar senhas fracas ou ignorar atualizações são atitudes que comprometem a segurança.
- Sabendo disso, golpistas aplicam engenharia social para aplicar golpes.

MANIPULAÇÃO HUMANA COMO PORTA DE ENTRADA

- A Engenharia Social é uma técnica usada por cibercriminosos para explorar vulnerabilidades humanas.
- Em vez de atacar sistemas diretamente, eles manipulam emoções como medo, curiosidade ou confiança para obter informações confidenciais.
- 90% dos golpes virtuais diários são resultado de engenharia social.

A ARTE DE INFLUENCIAR PESSOAS

- A Persuasão é usada para induzir decisões, esse conceito é fundamental para entender como golpes manipulam emoções.
- Golpistas aplicam seus 7 princípios (reciprocidade, compromisso, autoridade, prova social, contraste, escassez e simpatia) para manipular vítimas.

CONCEITOS GERAIS

A AMEAÇA INVISÍVEL

- Malware é qualquer software malicioso criado para causar danos, roubar dados ou comprometer sistemas.
- Pode se disfarçar como arquivos legítimos e se espalhar por downloads, anexos ou links.
- Existem vários tipos de malware, eles serão detalhados no decorrer dos slides.

O PODER DE RETRIBUIR

- O princípio da persuasão da Reciprocidade diz que as pessoas tendem a retribuir favores.
- Golpistas usam isso oferecendo algo e, em troca, pede dados pessoais.
- Exemplo:
  - Site falso oferecendo um brinde gratuito, pedindo dados pessoais para que a vítima receba o brinde.

A FORÇA DAS DECISÕES PASSADAS

- O princípio da persuasão do Compromisso diz que uma vez que as pessoas tomam decisões, elas tendem a mantê-las por coerência.
- Golpistas usam isso para induzir ações subsequentes.
- Exemplo:
  - Após aceitar um pequeno termo, o usuário é levado a aceitar permissões perigosas em um aplicativo.

O PESO DA APARÊNCIA DE PODER

- O princípio da persuasão da Autoridade diz que pessoas tendem a obedecer figuras que aparentam ter autoridade.
- Golpistas exploram isso através de uniformes, títulos ou linguagem técnica para passarem confiança.
- Exemplo:
  - Um e-mail falso assinado pelo "Diretor de segurança da empresa" solicitando atualização urgente de senha.

PRINCÍPIOS DA PERSUASÃO

O "EFEITO MANADA" DIGITAL

- O princípio da persuasão da Prova Social é a tendência de seguir o comportamento da maioria.
- Golpistas simulam prévias aprovações falsas da mesma prática aplicada à vítima a fim de ganhar sua confiança.
- Exemplo:
  - Uma página de produto falso exibe centenas de avaliações positivas falsas para induzir compras.

PRINCÍPIOS DA PERSUASÃO

MANIPULAÇÃO POR COMPARAÇÃO

- O princípio da persuasão do Contraste é usado para tornar uma opção mais atrativa ao compará-la com outra exageradamente ruim ou cara.
- Exemplo:
  - Um site mostra um produto por R$999,00 "riscado" e oferece por R$99,00 com tempo limitado.

A PRESSA COMO ARMA

- O princípio da persuasão da Escassez diz que quando algo parece raro ou limitado, sentimos urgência em agir.
- Golpistas usam isso para forçar decisões rápidas e impulsivas.
- Exemplo:
  - Mensagem: "Últimas 3 unidades! Oferta expira em 10 minutos!" - Induz clique em link malicioso.

CONFIANÇA GANHA COM CARISMA

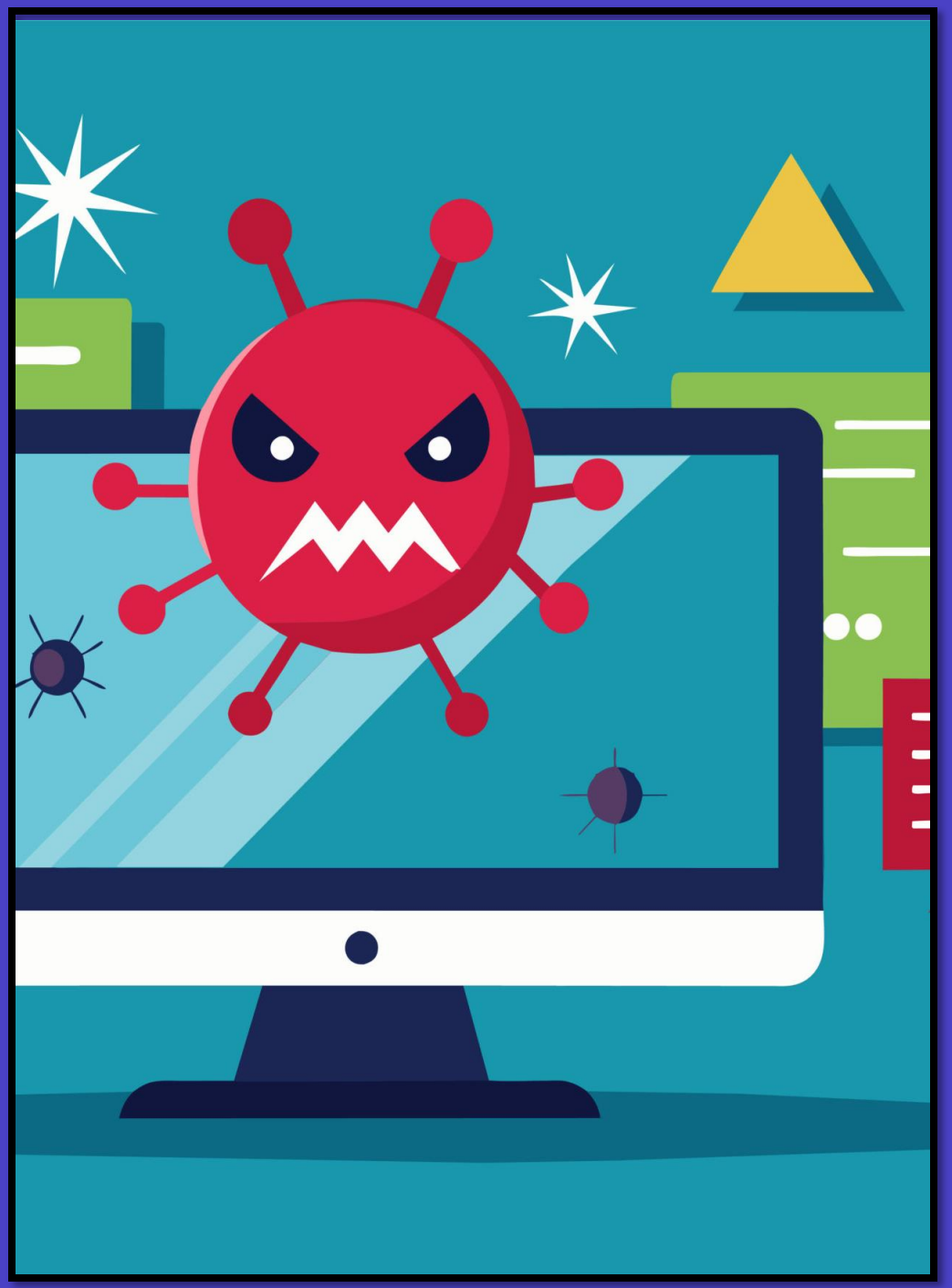
- O princípio da persuasão da Simpatia diz que tendemos a confiar em quem nos trata bem ou nos parece agradável.
- Golpistas simulam gentileza, empatia ou interesses em comum para conquistar vítimas.
- Exemplo:
  - Um golpista finge ser um colega de trabalho amigável em redes sociais para obter informações pessoais.

PRINCÍPIOS DA PERSUASÃO

CONTAMINÇÃO DIGITAL POR CONTATO

- Vírus são malwares que se replicam ao infectar outros arquivos.
- Dependem da ação do usuário para se espalhar, como abrir um arquivo contaminado.
- Exemplo:

  Um documento do Word infectado é aberto e espalha o vírus para outros arquivos do computador.



TIPOS DE MALWARE

PROPAGAÇÃO AUTOMÁTICA NA REDE

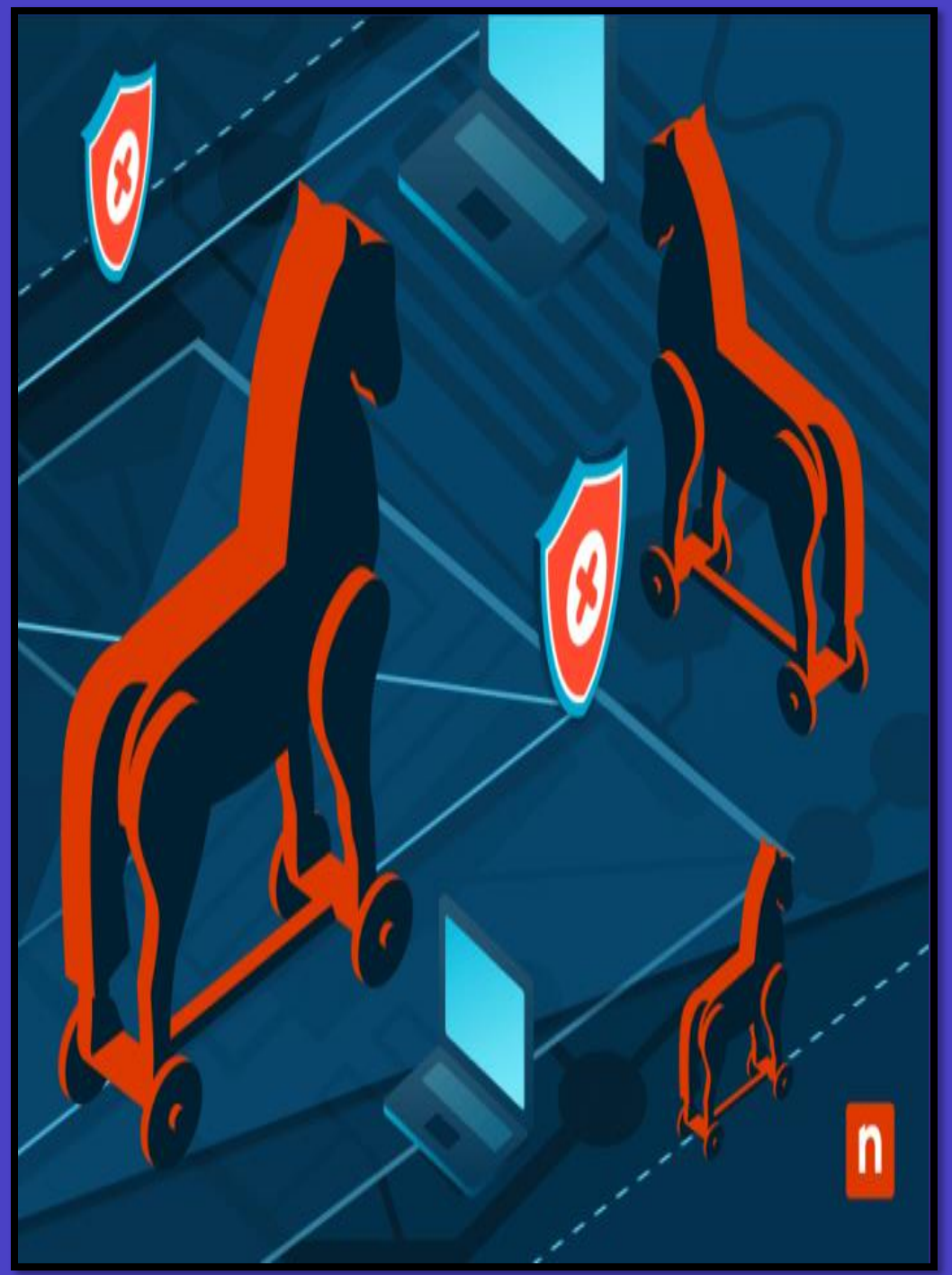
- Worms são malwares que se replicam automaticamente, sem necessidade de interação humana.
- Consomem recursos e podem causar lentidão ou travamentos.
- Exemplo:

  Um worm se espalha por e-mails, enviando cópias de si mesmo para todos os contatos da vítima.

O CAVALO DE TRÓIA DIGITAL

- Trojans se disfarçam como softwares legítimos, mas ao serem executados, abrem portas para invasores.
- O nome vem do mito grego do cavalo de Troia que foi usado para invadir uma cidade com uma técnica semelhante.
- Exemplo:

  Um jogo gratuito instala um trojan que permite controle remoto do computador por um hacker.



O ESPIÃO SILENCIOSO

- Um Spyware monitora secretamente as atividades do usuário, coletando dados como senhas, histórico de navegação e hábitos online.
- Exemplo:

  Um plugin de navegador aparentemente útil começa a rastrear tudo que o usuário digita.

SEQUESTRO DIGITAL COM RESGATE

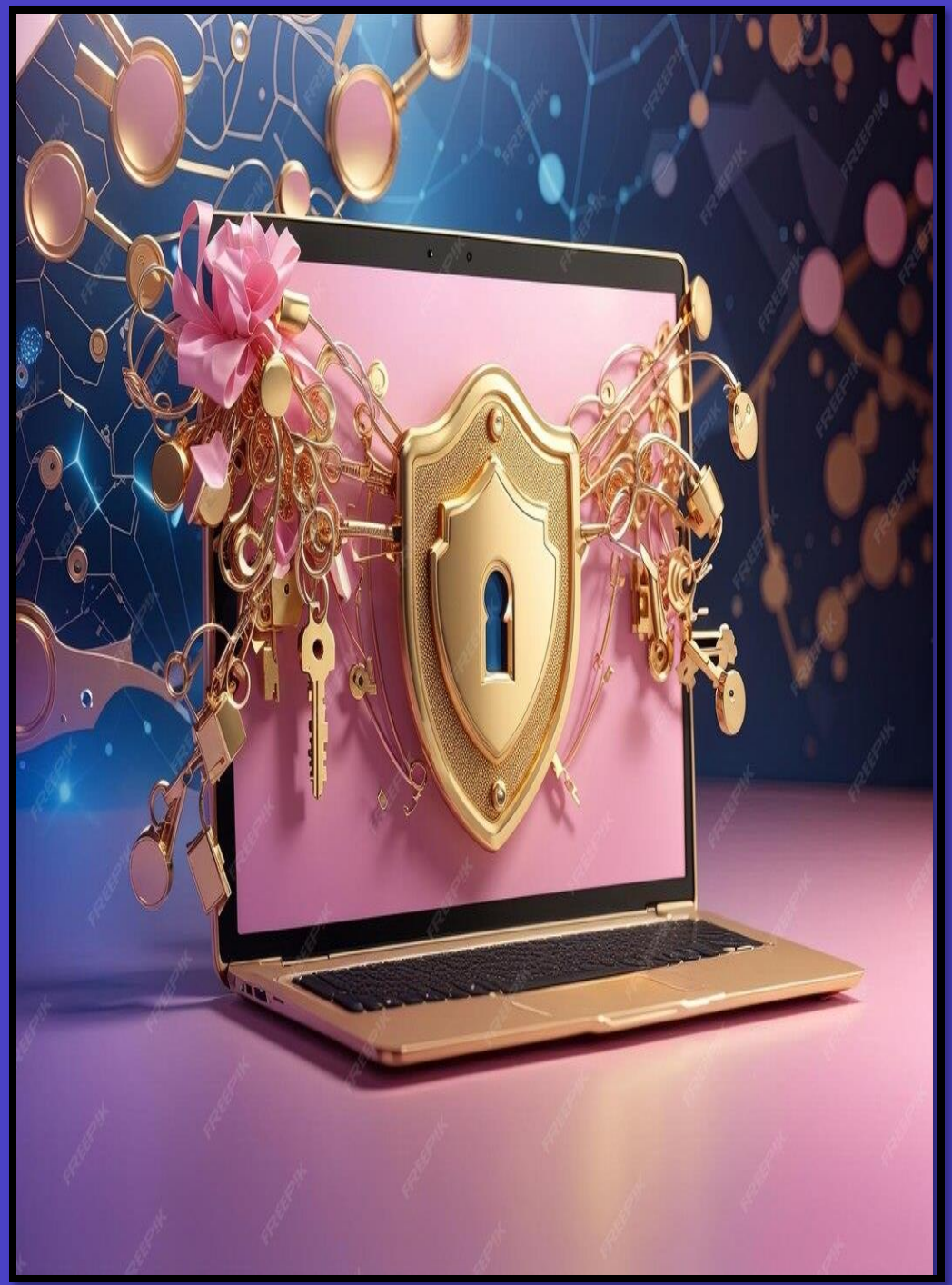
- O Ransomware criptografa arquivos e exige pagamento para liberá-los.
- É uma das ameaças mais graves, especialmente em ambientes corporativos.
- Exemplo:

  Uma empresa tem seus servidores bloqueados e recebe uma mensagem exigindo pagamento em criptomoedas.

CRIPTOGRAFIA MALICIOSA AVANÇADA

- O Criptomalware é uma variante do ransomware que usa algoritmos sofisticados para criptografar dados, tornando impossível o acesso sem a chave correta.
- Exemplo:

  Um arquivo aparentemente inofensivo inicia a criptografia de todo o disco rígido ao ser aberto.



PUBLICIDADE INDESEJADA E INVASIVA

- Adware exibe anúncios sem autorização e pode coletar dados de navegação.
- Frequentemente vem embutido em softwares gratuitos.
- Exemplo:

  Após instalar um programa gratuito, o navegador começa a abrir janelas de propaganda automaticamente.

A AMEAÇA OCULTA NO SISTEMA

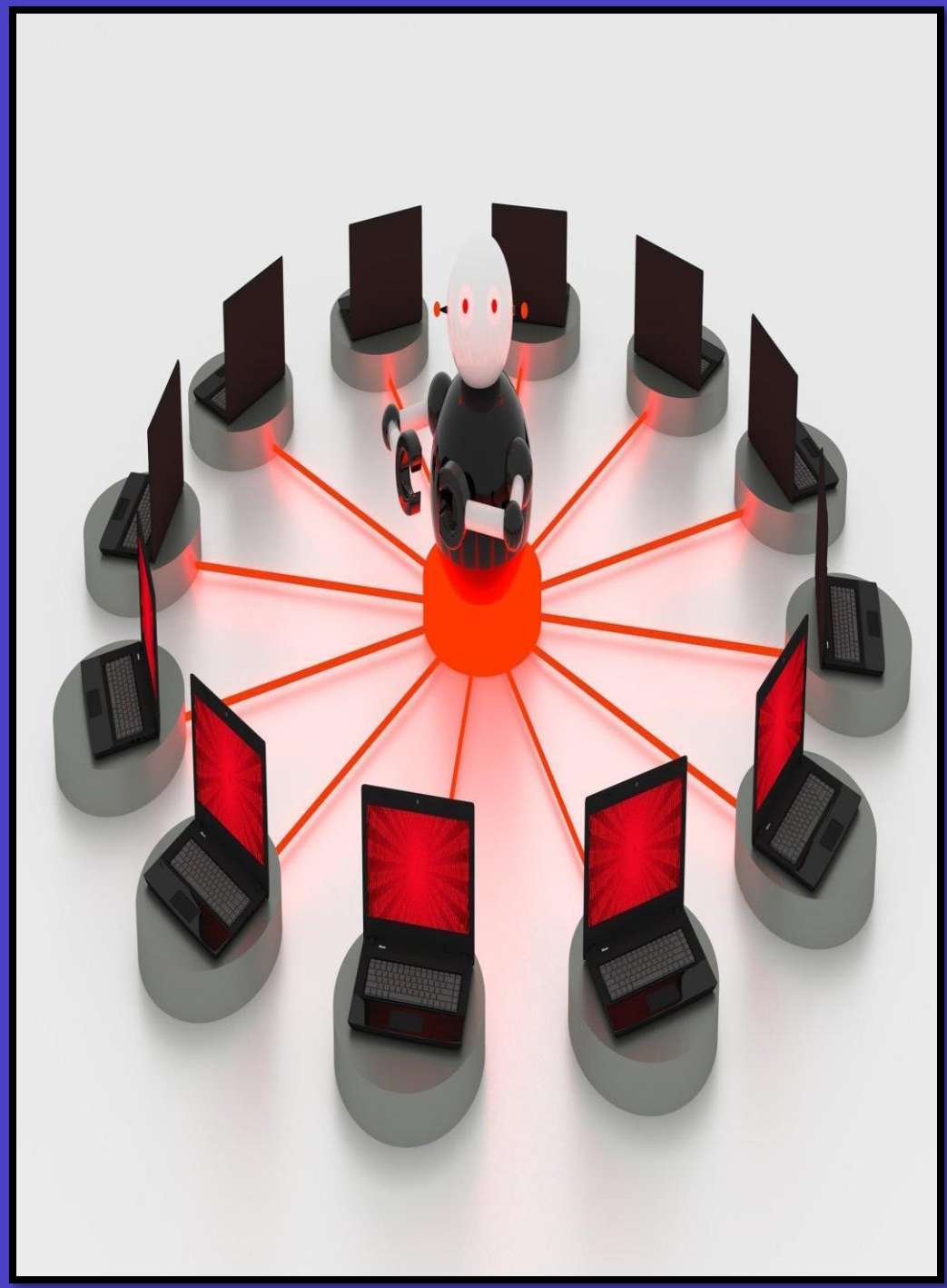
- Rootkits escondem a presença de malwares, atuando em níveis profundos do sistema.
- São difíceis de detectar e podem desativar antivírus.
- Exemplo:

  Um rootkit se instala junto com um driver de dispositivo e oculta um trojan do sistema de segurança.

EXÉRCITO DE MÁQUINAS ZUMBIS

- Botnets são redes de computadores infectados e controlados remotamente por um invasor.
- São usadas para ataques em massa, como DDoS (um ataque malicioso que visa sobrecarregar um servidor ou computador, esgotando seus recursos, como memória e processamento, tornando-o indisponível para os usuários).
- Exemplo:

  Milhares de máquinas infectadas são usadas para derrubar o site de uma empresa por sobrecarga de acessos.



FALSOS ALERTAS PARA INDUZIR MEDO

- Um Scareware simula ameaças no dispositivo para convencer o usuário a comprar softwares inseguros ou clicar em links perigosos.
- Exemplo:

  Pop-up diz “Seu computador está infectado! Clique aqui para resolver” – levando a um site fraudulento.

ESPIONAGEM POR TECLADO

- Um Keylogger registram tudo que o usuário digita, incluindo senhas e dados bancários.
- Podem ser softwares ou dispositivos físicos.
- Exemplo:

  Um programa instalado secretamente grava todas as teclas pressionadas e envia para o invasor.

ISCA DIGITAL PARA ROUBO DE DADOS

- O Phishing imita comunicações legítimas para enganar o usuário e obter dados sensíveis.
- Existem vários tipos dele e podem vir por e-mail, sites falsos, mensagens, etc.
- Mais adiante nos aprofundaremos em seus tipos.

TÉCNICAS DE APLICAÇÃO

CHANTAGEM DIGITAL COM CONTEÚDO ÍNTIMO

- Sextorsão envolve ameaças de divulgar imagens íntimas, muitas vezes obtidas por engenharia social ou invasão de dispositivos.
- Exemplo:

  Um golpista finge ser um interesse romântico, convence a vítima a enviar fotos e depois exige dinheiro para não divulgá-las.

TÉCNICAS DE APLICAÇÃO

O LIXO ELETRÔNICO DA INTERNET

- Spams são mensagens enviadas em massa, geralmente sem consentimento.
- Além de atrapalhar a produtividade, podem conter links maliciosos que levam a golpes ou instalação de malware.
- Exemplo:

  Um e-mail oferecendo “milhões de reais” leva o usuário a clicar em um link infectado.

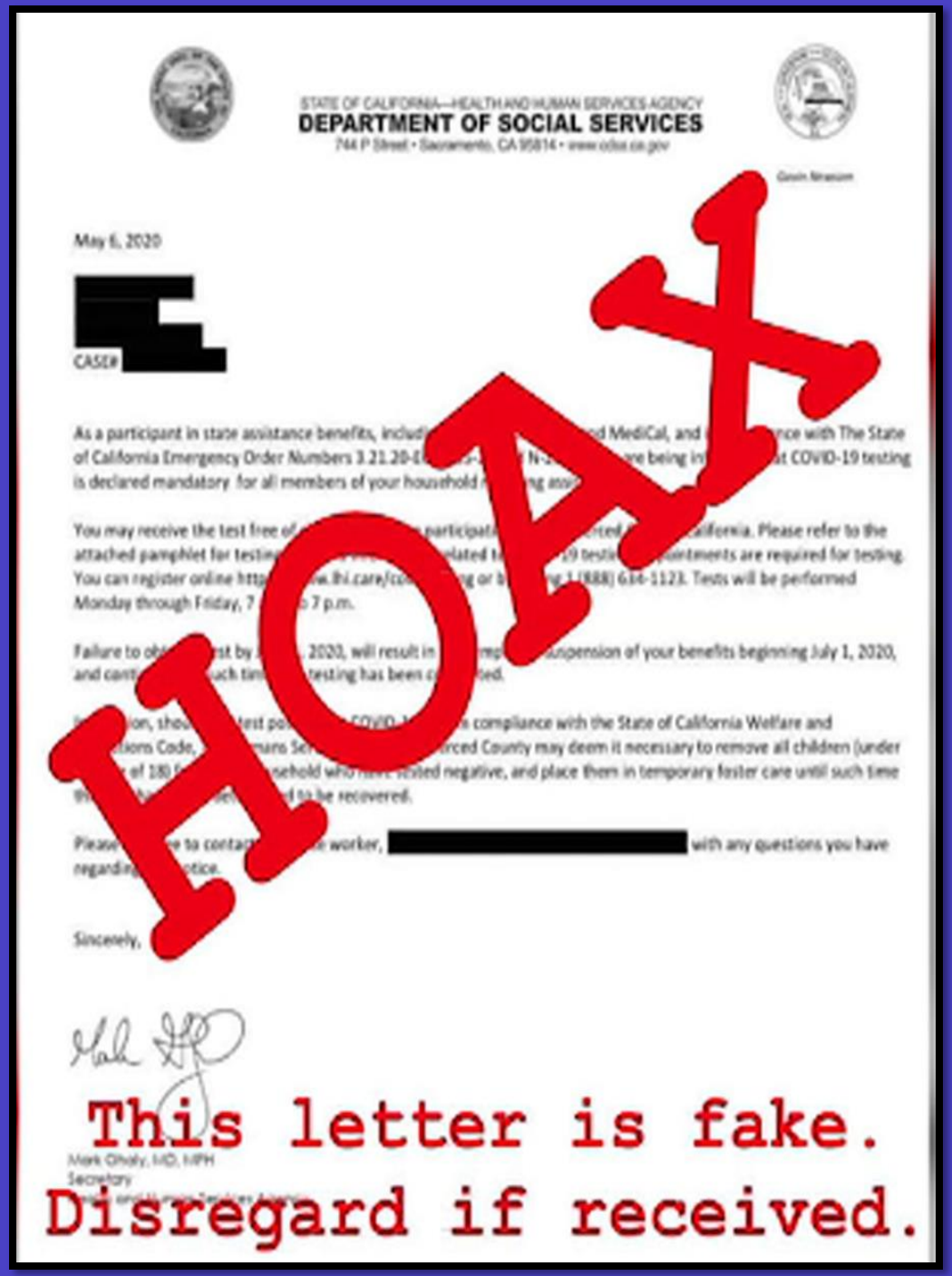
TÉCNICAS DE APLICAÇÃO

ALARMISMO DIGITAL SEM FUNDAMENTO

- Hoax Letters mensagens falsas com conteúdo alarmante que incentivam o compartilhamento em massa.
- Espalham desinformação e causam pânico.
- Exemplo:

  Mensagem viral diz que “o WhatsApp será pago amanhã” e pede que seja compartilhada com todos os contatos.

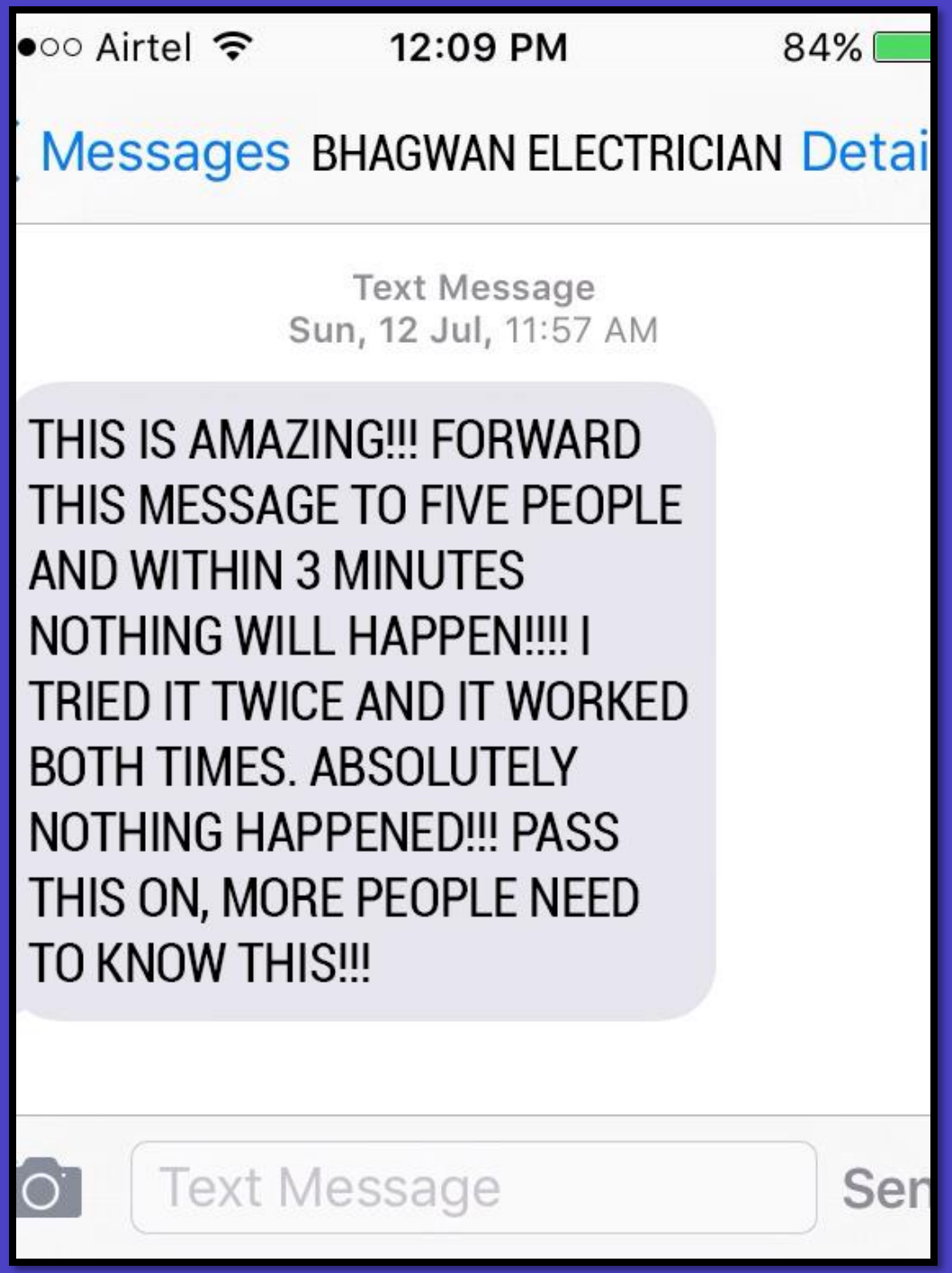
TÉCNICAS DE APLICAÇÃO



CORRENTES DIGITAIS DE SORTE OU AMEAÇA

- Chain Letters prometem benefícios ou ameaçam azar caso não sejam compartilhadas.
- Visam gerar tráfego ou viralização.
- Exemplo:

  "Compartilhe com 10 pessoas ou terá 7 anos de azar" – sem qualquer fundamento real.



TÉCNICAS DE APLICAÇÃO

GOLPE POR VOZ

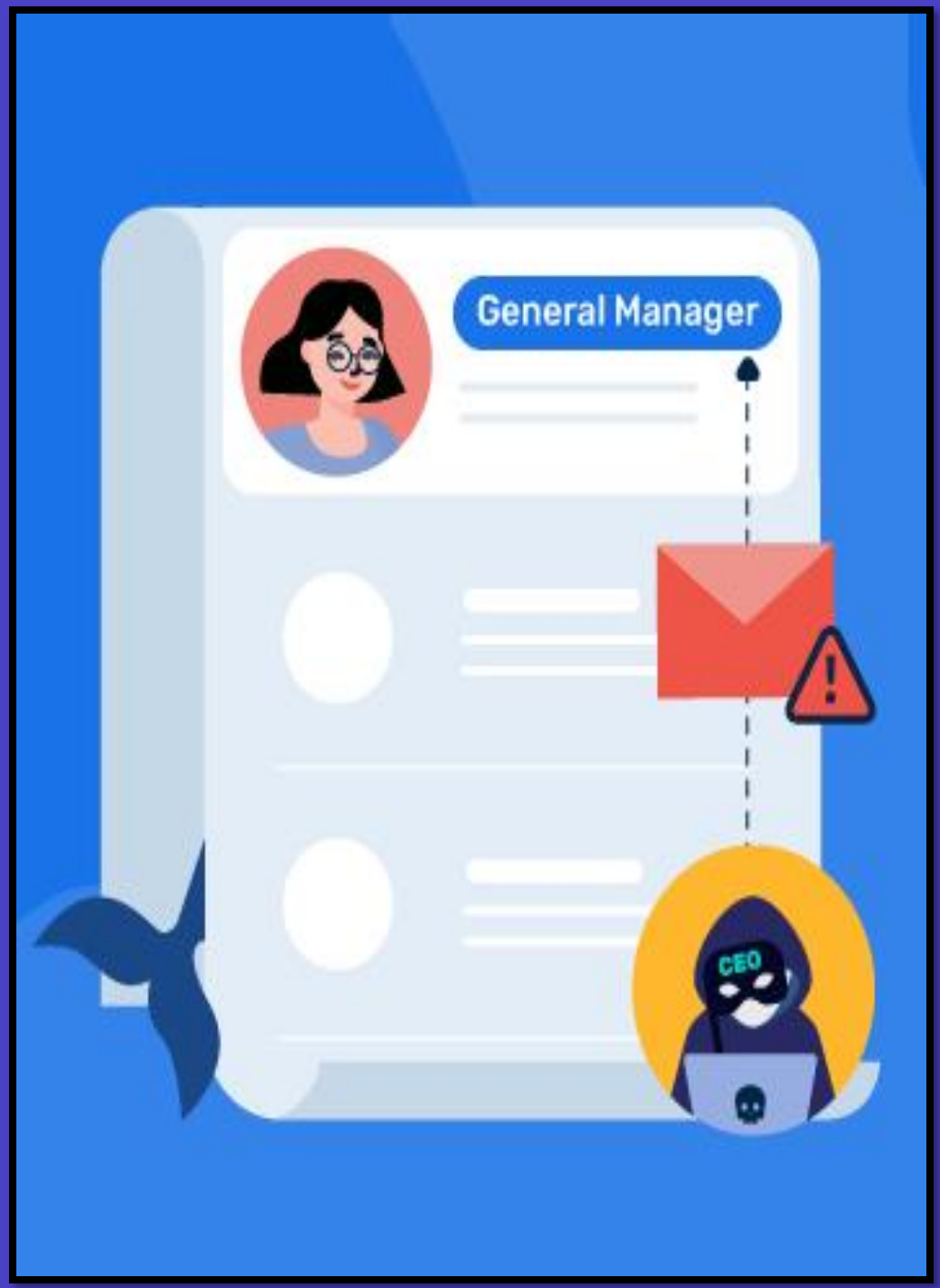
- Vishing é o phishing por telefone.
- O golpista finge ser de uma instituição confiável e tenta obter dados confidenciais.
- Exemplo:

  Ligação dizendo ser do banco solicita confirmação de dados para “evitar bloqueio da conta”.

CAÇA AOS GRANDES ALVOS

- Whaling é um tipo de phishing direcionado a executivos ou pessoas com acesso privilegiado.
- Os ataques são personalizados e discretos.
- Exemplo:

  E-mail falso direcionado ao CEO solicita transferência urgente de fundos.



GOLPE POR SMS OU MENSAGENS INSTANTÂNEAS

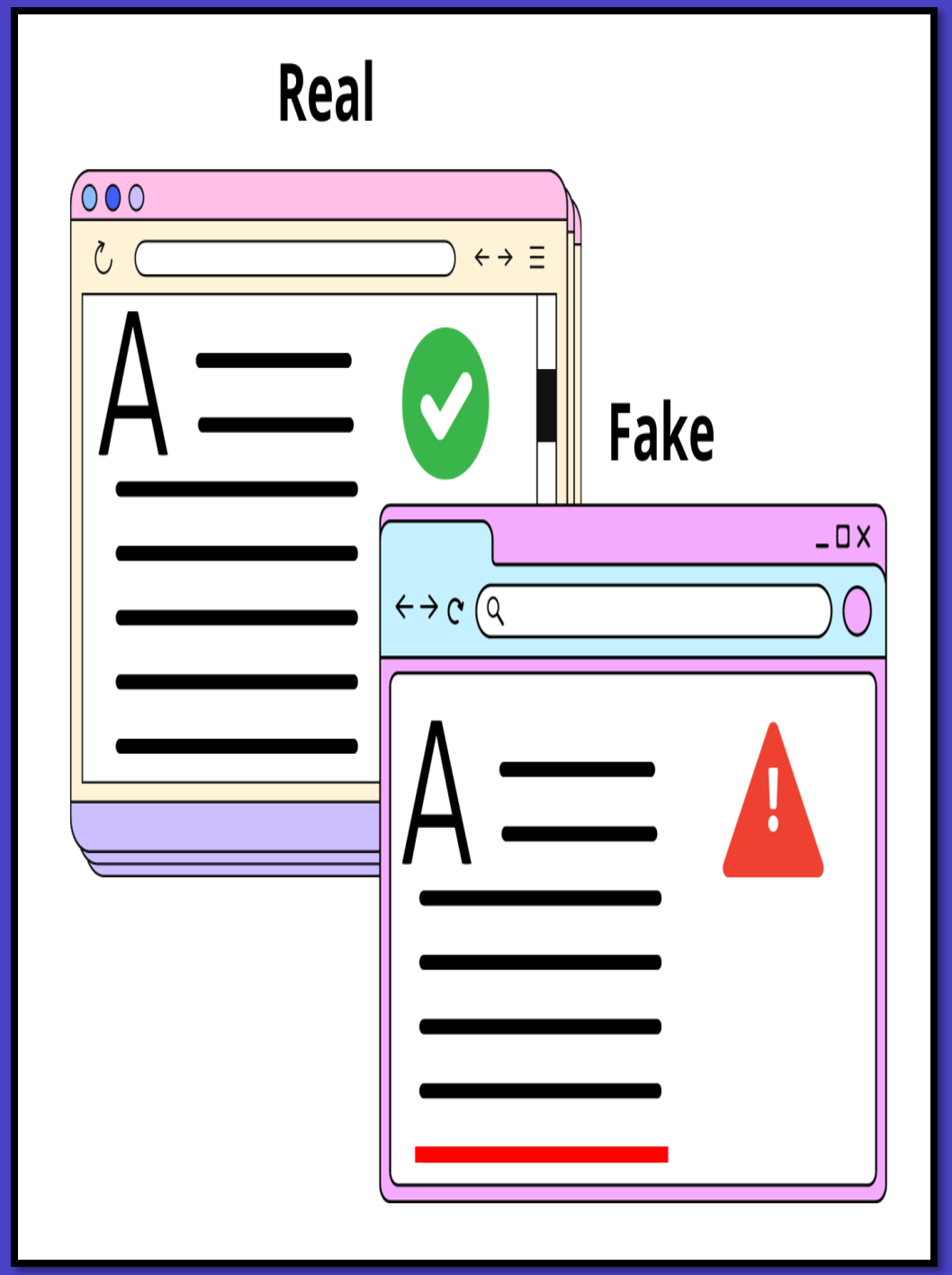
- Smishing usa mensagens curtas com links maliciosos, geralmente com tom alarmante ou promocional.
- Exemplo:

  SMS diz “Seu pacote está retido. Clique aqui para liberar” – levando a um site fraudulento.

CÓPIA PERFEITA COM INTENÇÃO MALICIOSA

- Clone phishing replica e-mails legítimos, substituindo links por versões maliciosas.
- Difícil de identificar.
- Exemplo:

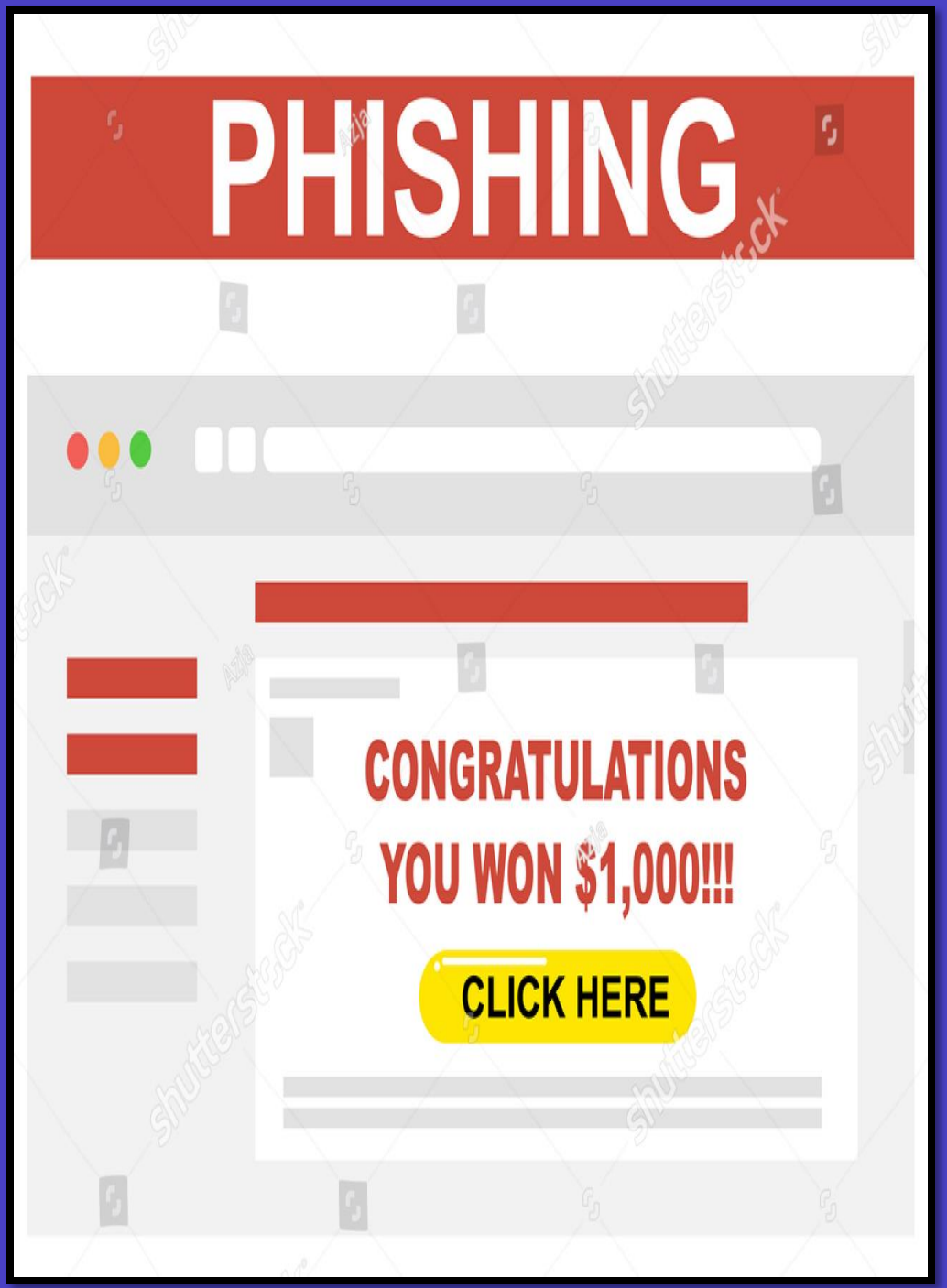
  Reenvio de e-mail real com link alterado para uma página falsa de login.



ISCAS DIGITAIS PARA ENGANAR

- Baiting usa recompensas falsas para atrair vítimas.
- Pode envolver brindes, curiosidade ou dispositivos físicos infectados.
- Exemplo:

  Um pendrive deixado propositalmente em um local público contém malware que se instala ao ser conectado.



TIPOS DE PHISHING

SITES FALSOS SEM SEGURANÇA

- HTTP phishing usa páginas fraudulentas sem criptografia (sem o “s” no “https”).
- É um sinal de que o site pode ser inseguro.
- Exemplo:

Um site de “banco” começa com http:// e solicita login.

ROTEIRO FALSO PARA OBTER CONFIANÇA

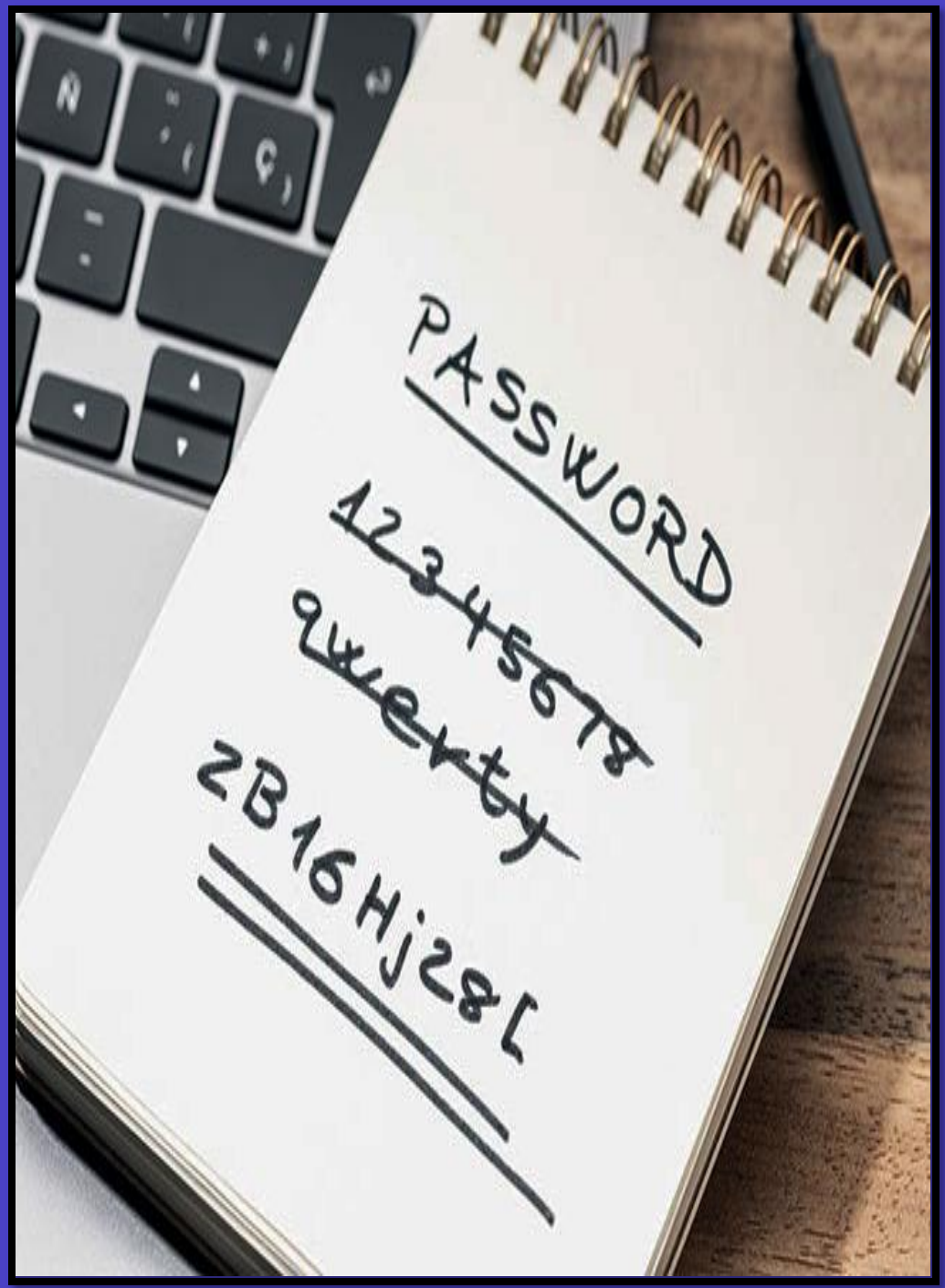
- Pretexting envolve criar uma história convincente para enganar.
- O golpista finge ser alguém confiável para extrair informações.
- Exemplo:

  Alguém se passa por funcionário do RH e solicita dados bancários para “atualização de cadastro”.

A PRIMEIRA LINHA DE DEFESA

- Senhas Fortes devem ser longas, com letras maiúsculas, minúsculas, números e símbolos.
- Evite dados pessoais e nunca repita senhas.
- Exemplo:

  Senha segura: `T!gr3s#2025@L!vros` – difícil de adivinhar e única para cada serviço.



MEIOS DE PREVENÇÃO

DUPLA PROTEÇÃO PARA ACESSO SEGURO

- Autenticação em Dois Fatores combina senha com outro fator (SMS, app, biometria).
- Mesmo que a senha seja roubada, o acesso é bloqueado sem o segundo fator.
- Exemplo:

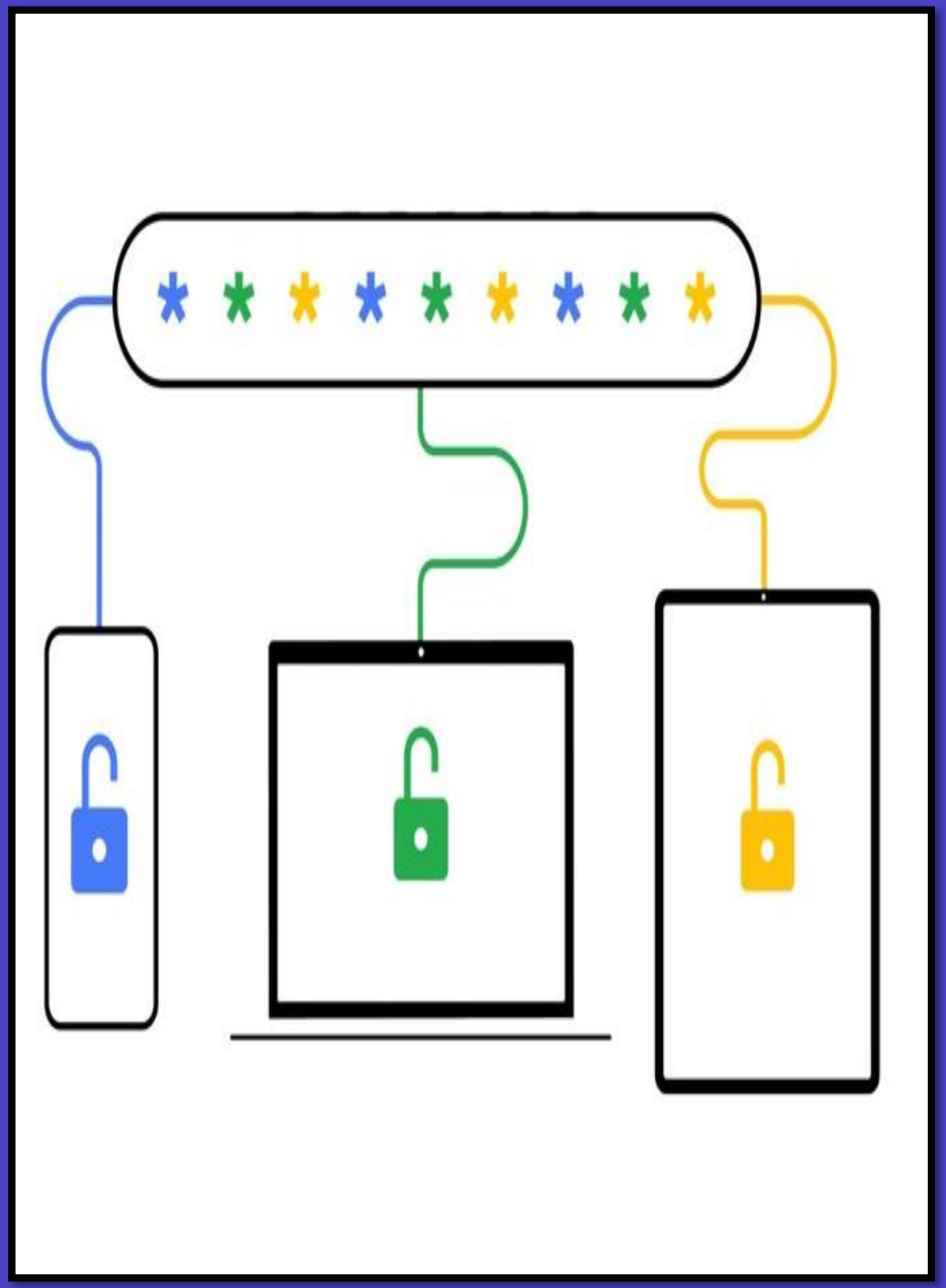
  Após digitar a senha, o sistema exige um código enviado por SMS para liberar o acesso.

MEIOS DE PREVENÇÃO

SEGURANÇA E PRATICIDADE NA GESTÃO DE CREDENCIAIS

- Gerenciador de Senhas permite armazenar senhas fortes e únicas para cada serviço.
- Evita-se reutilização e facilita o uso seguro.
- Exemplo:

  O usuário acessa o gerenciador com uma senha mestra e copia senhas complexas para cada site.



MEIOS DE PREVENÇÃO

CONHECIMENTO COMO DEFESA

- A Educação Digital propõe treinamentos e conscientização para reduzir falhas humanas.
- Compartilhar boas práticas fortalece toda a equipe.
- Exemplo:

  Empresa realiza workshops mensais sobre segurança digital e simulações de phishing.

MEIOS DE PREVENÇÃO

CORRIGIR PARA PREVENIR

- Atualizações de Sistema corrigem falhas que podem ser exploradas por cibercriminosos.
- Ignorar atualizações deixa o sistema vulnerável.
- Exemplo:

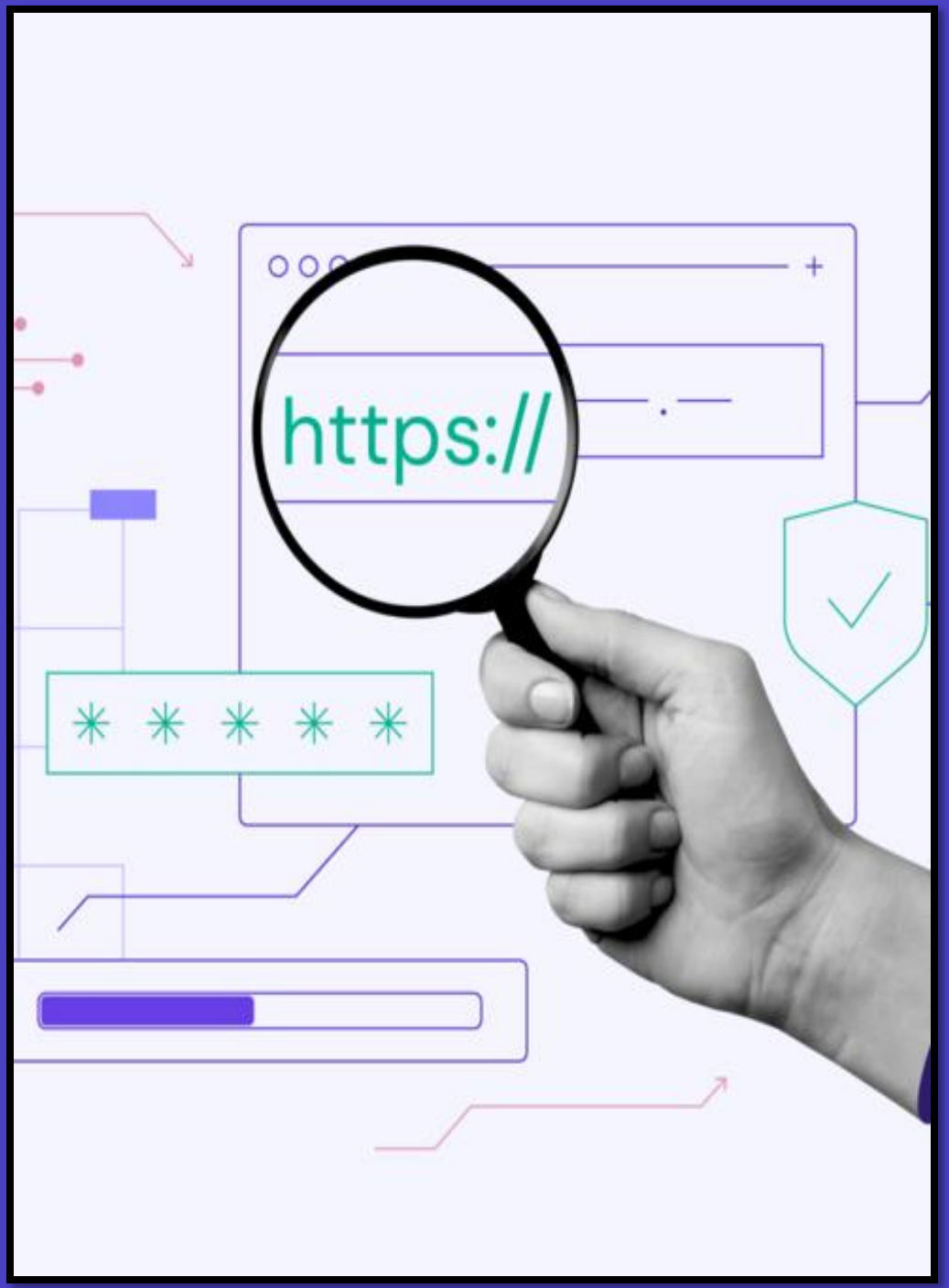
  Um patch de segurança é lançado para corrigir uma brecha que permitia acesso remoto não autorizado.

MEIOS DE PREVENÇÃO

ATENÇÃO ANTES DE CLICAR

- Verificar Links antes de clicar, consiste em passar o mouse sobre o link para ver o destino real.
- Links suspeitos podem ter erros sutis ou redirecionamentos falsos.
- Exemplo:

  Ao receber um e-mail do “banco”, o usuário verifica o link e percebe que leva a `http://seguranca-banco123.com`, um site falso.



MEIOS DE PREVENÇÃO