aizen

GUIA PRÁTICO DE

PROTEÇÃO CONTRA GOLPES DIGITAIS

Como identificar tentativas de *phishing*, URLs falsas e proteger suas informações na internet

- Aprenda a identificar sinais de golpes e fraudes online
- Entenda como domínios, URLs e protocolos funcionam
- Conheça as técnicas usadas por criminosos para enganar
- Adote boas práticas e proteja seus dados pessoais e corporativos
- Ideal para usuários e empresas que levam segurança a sério

INFORMAÇÃO É A SUA **MELHOR DEFESA.**

aizen

APRESENTAÇÃO

Os golpes digitais evoluíram.
O que antes era fácil de identificar, hoje é cada vez mais sofisticado, personalizado e convincente.

Conhecimento é a sua melhor defesa.

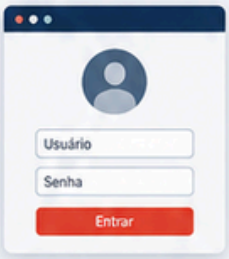
A EVOLUÇÃO DOS GOLPES DIGITAIS

2010 — E-MAILS SIMPLES

Mensagens mal escritas, com erros de português e links suspeitos.

Fácil de identificar por usuários atentos.

2015 — PÁGINAS FALSAS SIMPLES



Sites falsos com layouts básicos, imitando marcas conhecidas.

Atenção ao domínio já fazia diferença.

2020 — SITES IDÊNTICOS AOS ORIGINAIS

Páginas muito bem construídas, com HTTPS válido e aparência profissional.

Difícil identificar sem análise técnica do domínio e do contexto.

2025+ — IA, DEEPFAKES E PHISHING PERSONALIZADO

Mensagens altamente personalizadas com IA, voz, vídeos e informações reais sobre a vítima.

Golpes cada vez mais convincente e difíceis de detectar.

O phishing continua sendo uma das principais portas de entrada para ataques e violações de dados em empresas de todos os portes.

- Afeta usuários e organizações no mundo inteiro
- Pode causar prejuízos financeiros, vazamento de dados e perda de reputação
- A conscientização é a ferramenta mais eficaz contra esses ataques

Este guia foi criado para ajudar você a entender como esses golpes funcionam e como se proteger de forma prática e eficiente.

aizen

por **Fernando Prazeres**
Head de Offensive

Todos os dias, milhões de pessoas recebem e-mails, mensagens e notificações aparentemente legítimas solicitando alguma ação urgente: Atualizar uma senha, confirmar uma compra, verificar uma entrega ou validar um acesso.

Muitas dessas mensagens são fraudulentas.

O problema é que os golpes digitais evoluíram. Hoje, criminosos utilizam páginas praticamente idênticas às originais, certificados HTTPS válidos, logotipos legítimos e técnicas avançadas de engenharia social para enganar usuários.

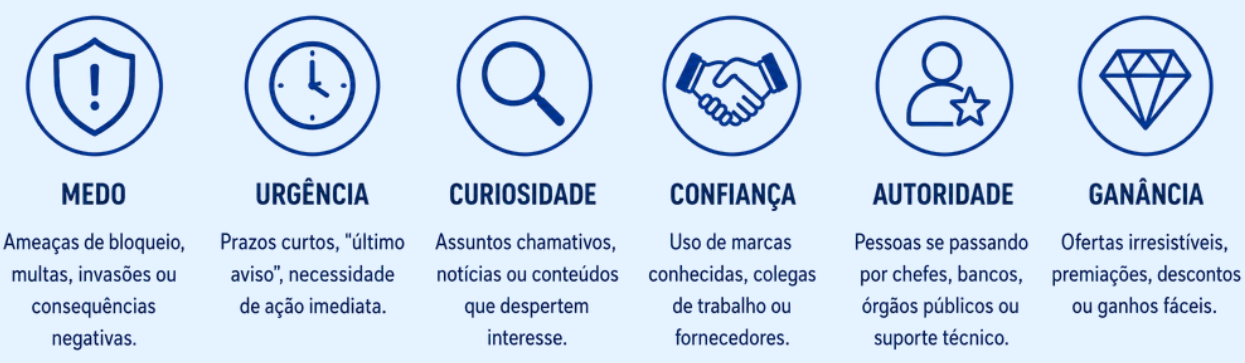
Este guia foi criado para ajudar usuários e empresas a compreender como esses golpes funcionam e como identificá-los antes que causem prejuízos.

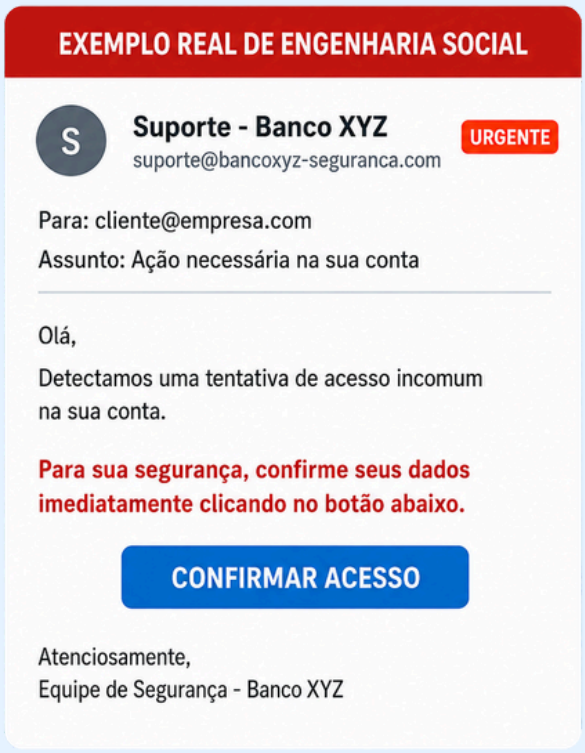
O que é Engenharia Social?

Antes de entender o *phishing*, é importante compreender o conceito que está por trás dele.
Engenharia Social é a manipulação psicológica de pessoas com o objetivo de obter informações, acesso ou executar ações que beneficiem o atacante.

Em vez de atacar diretamente computadores e sistemas, o criminoso explora comportamentos humanos.

EMOÇÕES MAIS EXPLORADAS





O que é *Phishing*?

Phishing é uma técnica de fraude digital baseada em Engenharia Social. O criminoso se passa por uma pessoa, empresa ou instituição legítima para induzir a vítima a fornecer informações sensíveis. Essas informações podem incluir:

- Usuários e senhas
- Dados bancários
- Informações pessoais
- Dados corporativos
- Códigos de autenticação.

CANAIS MAIS UTILIZADOS

Na maioria dos casos, o **objetivo final** é roubar credenciais ou direcionar a vítima para uma página falsa

Como funciona a Internet?

Para compreender diversos golpes digitais, é importante conhecer alguns conceitos básicos.

Quando você acessa um site:

a. Digita um endereço.
b. Seu computador procura o servidor responsável.
c. A conexão é estabelecida.
d. O conteúdo do site é carregado.

Os criminosos exploram exatamente esse processo para criar páginas falsas que parecem legítimas.

O que é um "Domínio"?

Um domínio é o endereço de um site na internet.

Da mesma forma que você utiliza um endereço para encontrar uma casa, você utiliza um domínio para encontrar um site.

O que é um "DNS"?

DNS significa *Domain Name System*.
Ele funciona como uma agenda telefônica da internet. Quando você digita: www.google.com, O DNS converte esse nome em um endereço IP utilizado pelos computadores para localizar o servidor correto.

O que é uma credencial?

Credenciais são as informações usadas para provar sua identidade e obter acesso a sistemas, aplicações, contas e dados

TIPOS DE CREDENCIAIS

USUÁRIO E SENHA
Combinação tradicional usada para autenticar usuários em sistemas e e-mails.

TOKENS DE ACESSO
Códigos temporários gerados por aplicativos ou dispositivos físicos (2FA/MFA).

CERTIFICADOS DIGITAIS
Utilizados para autenticar identidades e garantir comunicações seguras (ex.: TLS).

CHAVES DE API
Permitem que aplicações se comuniquem entre si de forma autenticada.

PINS E BIOMETRIA
Utilizados em dispositivos móveis ou físicos para validação de identidade.

O RISCO DAS CREDENCIAIS COMPROMETIDAS

- Acesso não autorizado a sistemas e dados sensíveis.
- Movimentações financeiras indevidas.
- Vazamento de informações sigilosas.
- Instalação de malware e ransomware.
- Prejuízos financeiros e danos à reputação da empresa.

BOAS PRÁTICAS PARA PROTEGER SUAS CREDENCIAIS

- Use senhas fortes e únicas para cada serviço.
- Ative a autenticação multifator (MFA) sempre que possível.
- Nunca compartilhe suas credenciais, nem por e-mail ou mensagem.
- Utilize gerenciadores de senhas confiáveis.
- Revogue acessos de usuários que não fazem mais parte da equipe.
- Monitore o uso de contas privilegiadas.
- Treine sua equipe continuamente sobre segurança da informação.

O que é Autenticação Multifator (MFA)?

É uma camada extra de segurança que exige dois ou mais fatores de verificação para confirmar a identidade de um usuário antes de conceder acesso a sistemas e informações.

OS 3 TIPOS DE FATORES DE AUTENTICAÇÃO

1 ALGO QUE VOCÊ SABE
Conhecimento

- Senha
- PIN
- Resposta secreta

Exemplo: sua senha de acesso.

2 ALGO QUE VOCÊ TEM
Posse

- Código gerado por aplicativo
- Token físico
- SMS ou e-mail com código

Exemplo: código de 6 dígitos do app autenticador.

3 ALGO QUE VOCÊ É
Inerência

- Impressão digital
- Reconhecimento facial
- Reconhecimento de íris

Exemplo: sua digital ou reconhecimento facial no dispositivo.

COMO FUNCIONA NA PRÁTICA

1. **Usuário informa seu usuário e senha.**
2. **O sistema solicita o segundo fator de autenticação.**
3. **O usuário fornece o código ou confirma a solicitação.**
4. **Acesso concedido com segurança.**

MFA é mais do que uma opção. Atualmente, é uma necessidade para proteger o que realmente importa.

SEM MFA, VOCÊ ESTÁ EM RISCO!

- Senhas podem ser roubadas por phishing, malware ou vazamentos.
- Ataques de força bruta podem comprometer contas fracas.
- Contas comprometidas podem gerar prejuízos financeiros, vazamento de dados e danos à reputação.

ADOTE MFA NA SUA EMPRESA

Implementar MFA é uma das formas mais eficazes e acessíveis de proteger sua organização contra ataques. Comece pelos acessos mais críticos e expanda para todos os usuários.

Segurança em camadas é segurança de verdade!

O que é *Certificado Digital*?

O certificado digital é um arquivo eletrônico que funciona como uma identidade para sites na internet. Ele permite que o navegador verifique se o site **é quem afirma ser** e se a conexão está protegida com criptografia (HTTPS).

O CADEADO NÃO SIGNIFICA QUE O SITE É CONFIÁVEL

Muitos acreditam que, se o site tem cadeado (HTTPS), ele é seguro. Isso não é verdade! O certificado apenas confirma a identidade do site, mas não o conteúdo ou a intenção dele.

Golpistas também conseguem certificados digitais válidos para sites falsos.

Abaixo, temos 2 exemplos de sites, porém, apenas um é confiável.

Ao lado, indicamos o passo a passo para verificar se um site possui o certificado ou não.

O que é HTTP e *HTTPS*?

Ao acessar um site, você verá normalmente:

- http://
- https://

O HTTPS significa que a comunicação entre seu dispositivo e o servidor está criptografada. **Isso protege os dados durante a transmissão.** No entanto, muitas pessoas acreditam que o cadeado do navegador garante que um site é confiável.

Isso não é verdade.

O HTTPS apenas indica que a conexão está protegida. Um site falso também pode utilizar HTTPS. Por isso, o domínio continua sendo o elemento mais importante a ser verificado.

Como ler uma URL corretamente?

Esta é uma das habilidades mais importantes para identificar golpes.

Observe a URL abaixo:
https://login.microsoft.seguranca-verificacao.net/login

Ela pode parecer legítima à primeira vista. Porém, vamos analisá-la com calma:

As técnicas mais utilizadas para criar URLs falsas, e confundir o usuário, são as seguintes:

- Troca de caracteres
  - https://microsoft.com
  - https://micr0soft.com (substitui a letra O por zero)
- Palavras adicionais;
- Subdomínios enganosos;
- Erros de digitação
  - https://goooogle.com
  - https://amazom.com

EXEMPLOS COMPARATIVOS

URL	DOMÍNIO VERDADEIRO	EXPLICAÇÃO	LEGÍTIMO?
https://account.microsoft.com	microsoft.com	Domínio oficial da Microsoft.	✓
https://account.microsoft.com.seguranca-login.net	seguranca-login.net	O domínio verdadeiro é "seguranca-login.net", não a Microsoft.	✗
https://login.microsoft.com	microsoft.com	Subdomínio oficial dentro do domínio da Microsoft.	✓
https://microsoft-login.net	microsoft-login.net	Domínio criado pelo atacante para se passar pela Microsoft.	✗
https://seguranca.verificacao-banco.com.br/login	verificacao-banco.com.br	O domínio verdadeiro é do atacante.	✗

Como os golpistas escolhem suas vítimas?

Muitas pessoas acreditam que os golpes são enviados aleatoriamente. Nem sempre. Criminosos frequentemente utilizam informações públicas disponíveis em:

- LinkedIn
- Redes sociais
- Sites corporativos
- Vazamentos de dados
- Notícias públicas
- Cadastros expostos na internet

Quanto mais informações conseguem obter, mais convincente será o golpe.

Por isso, ataques modernos costumam conter nomes reais, cargos, empresas e até referências a projetos ou fornecedores legítimos.

Como identificar um e-mail suspeito?

E-mails continuam sendo uma das principais portas de entrada para ataques cibernéticos.
Saber identificá-los ajuda a evitar a fraude que normalmente vem na forma de roubo de dados, prejuízos financeiros e a instalação de *malware* no dispositivo.

Antes de clicar em qualquer link, verifique:

EXEMPLO REAL: COMPARE

E-MAIL LEGÍTIMO

De:	notificacoes@bancooficial.com.br
Assunto:	Aviso de segurança da sua conta
Saudação:	Olá, João Silva
Link:	https://www.bancooficial.com.br/seguranca

Características:
- Domínio oficial
- Linguagem clara e profissional
- Sem pressão para ação imediata
- Design padronizado da marca

E-MAIL SUSPEITO

De:	seguranca@banco-oficial-atualiza.com
Assunto:	URGENTE! Sua conta será bloqueada
Saudação:	Prezado cliente
Link:	http://bit.ly/atualize-sua-conta

Características:
- Domínio estranho
- Linguagem ameaçadora
- Link encurtado
- Erros de português e formatação

Em resumo, golpistas usam engenharia social para criar e-mails que parecem reais e confiáveis. Atenção ao detalhes é essencial para não cair em armadilhas.

VERIFICAÇÕES RÁPIDAS ANTES DE AGIR

1. Confira o remetente completo.
2. Analise o assunto com atenção.
3. Passe o mouse sobre os links (sem clicar).
4. Desconfie de anexos inesperados.
5. Em caso de dúvida, não clique e não responda.

Regra de ouro: se algo parece estranho, provavelmente é.

O que fazer se você foi vítima

Mesmo com todos os cuidados, pode acontecer de cair em um golpe. O mais importante, neste caso, é agir rápido para minimizar os danos e evitar que o problema aumente. E o mais importante:

NÃO ENTRE EM PÂNICO

Respire fundo e siga os passos. Agir com calma e rapidez é essencial para reduzir os impactos.

Siga o passo a passo abaixo do que fazer

O QUE FAZER DE ACORDO COM A SITUAÇÃO

CLICOU EM UM LINK SUSPEITO
→ Altere suas senhas e verifique se houve acesso indevido.

INFORMOU SENHA
→ Altere a senha imediatamente e ative o 2FA.

INFORMOU DADOS DE CARTÃO
→ Contate seu banco ou operadora do cartão imediatamente. Solicite bloqueio e monitore transações.

BAIXOU UM ARQUIVO
→ Desconecte do Wi-Fi, execute uma verificação com antivírus e avise o time de TI.

INFORMOU DADOS PESSOAIS
→ Monitore sinais de uso indevido (SPAM, tentativas de fraude) e, se necessário, registre um boletim de ocorrência.

O QUE NÃO FAZER

- Não forneça mais informações ao golpista.
- Não clique em novos links ou anexos.
- Não tente "resolver sozinho" sem orientação.
- Não ignore o incidente ou tenha vergonha de comunicar.
- Não reutilize senhas comprometidas.

COMUNIQUE E REGISTRE

Informe o incidente ao seu time de TI, Segurança da Informação ou seu gestor.

Se houver prejuízo financeiro ou uso indevido de dados, registre um boletim de ocorrência na delegacia (física ou online).

Isso ajuda nas investigações e na proteção de outras pessoas.

Checklist final contra Golpes Digitais

Use este checklist como guia rápido no seu dia a dia. Construir o hábito de pequenas verificações podem evitar grandes problemas

REGRAS DE OURO DA SEGURANÇA

- **Desconfie sempre**
- **Verifique antes de agir**
- **Proteja suas informações**
- **Comunique e compartilhe**
- **Mantenha hábitos seguros**

CHECKLIST RÁPIDO

1 REMETENTE CONFIÁVEL?

O e-mail ou mensagem é de alguém ou empresa que você conhece?

☐ Sim ☐ Não ☐ Não sei

2 ENDEREÇO CORRETO?

O link ou site tem o endereço correto e sem alterações?

☐ Sim ☐ Não ☐ Não sei

3 HTTPS E CADEADO?

O site usa HTTPS e o cadeado está presente?

☐ Sim ☐ Não ☐ Não sei

4 CONTEÚDO FAZ SENTIDO?

A mensagem está coerente e sem erros ou promessas exageradas?

☐ Sim ☐ Não ☐ Não sei

5 LINKS E ANEXOS?

Passe o mouse sobre os links e verifique o destino real. Anexos são esperados?

☐ Sim ☐ Não ☐ Não sei

6 SOLICITA DADOS PESSOAIS?

Estão pedindo senhas, dados de cartão ou informações pessoais? Isso é realmente necessário?

☐ Sim ☐ Não ☐ Não sei

7 SENSAÇÃO DE URGÊNCIA?

A mensagem pede ação imediata, ameaça ou cria sensação de pânico?

☐ Sim ☐ Não ☐ Não sei

8 FONTE OFICIAL CONFIRMADA?

Confirme a informação por um canal oficial (site, telefone ou aplicativo da empresa).

☐ Sim ☐ Não ☐ Não sei

9 DISPOSITIVO SEGURO?

Estou usando um dispositivo atualizado e protegido (antivírus ativo)?

☐ Sim ☐ Não ☐ Não sei

10 REDE CONFIÁVEL?

Estou em uma rede segura e confiável para acessar informações sensíveis?

☐ Sim ☐ Não ☐ Não sei

11 DUVIDOU? NÃO CLICOU!

Se algo parece estranho, você não clicou e não informou nenhum dado?

☐ Sim ☐ Não ☐ Não sei

12 LEMBRE-SE

A tecnologia protege, mas é você quem decide. Informação e atenção são suas melhores defesas.

Na dúvida, pause. Verifique. Proteja-se e proteja sua empresa.

Conclusão

A maioria dos golpes digitais modernos não depende de vulnerabilidades técnicas complexas. Eles exploram comportamentos humanos.

Por isso, a conscientização continua sendo uma das camadas de proteção mais importantes para usuários e organizações.

Alguns segundos de análise podem evitar o comprometimento de contas, perdas financeiras e vazamentos de informações sensíveis.