CIBERSEGURANÇA

Fundamentos da Cibersegurança

PROTEJA SEU MUNDO DIGITAL

Imagine perder acesso a todas as suas contas online ou ter suas informações financeiras comprometidas.
A cibersegurança não é apenas uma preocupação técnica é uma necessidade para proteger você.

Em um mundo onde nossas vidas estão cada vez mais integradas à tecnologia, desde compras online até a comunicação com amigos e familiares, a segurança digital se tornou uma prioridade.

CIBERSEGURANÇA

Descubra por que a cibersegurança é essencial para proteger suas informações no mundo digital

CIBERSEGURANÇA

Cibersegurança é o conjunto de práticas, tecnologias e processos projetados para proteger sistemas, redes e dados contra ataques digitais. É como um escudo que impede invasores de acessar informações sensíveis e comprometer sua privacidade.

Por que é importante? No mundo digital, nossos dados são ativos valiosos. Desde informações bancárias até fotos pessoais, tudo pode ser alvo de ataques, o que torna a segurança um investimento indispensável.

02

SEU PRIMEIRO ESCUDO

Aprenda a criar senhas que realmente protejam suas contas e dados

CRIAÇÃO DE SENHAS FORTES

Senhas são a primeira linha de defesa na cibersegurança. Uma boa senha não é apenas longa, mas também única. Combinar letras maiúsculas e minúsculas, números e símbolos dificulta que hackers adivinhem ou quebrem sua senha por meio de programas automatizados.

Exemplo real: Rafael, um empresário, perdeu acesso ao seu e-mail porque reutilizava a mesma senha simples em vários serviços. Um vazamento em um site comprometeu sua conta principal.

03

PHISHING

As armadilhas mais comuns usadas por cibercriminosos

PHISHING: IDENTIFICANDO E EVITANDO ARMADILHAS

Phishing é uma prática maliciosa em que cibercriminosos enviam mensagens falsas, muitas vezes disfarçadas como comunicações legítimas de bancos, empresas ou organizações confiáveis. O objetivo é enganar as vítimas para que revelem informações sensíveis, como senhas, dados bancários ou números de cartões de crédito. Essas mensagens podem chegar por e-mail, SMS, redes sociais ou até aplicativos de mensagens instantâneas.

A melhor defesa contra o **phishing** é desconfiar de mensagens não solicitadas, verificar sempre a autenticidade do remetente e nunca clicar em links suspeitos.

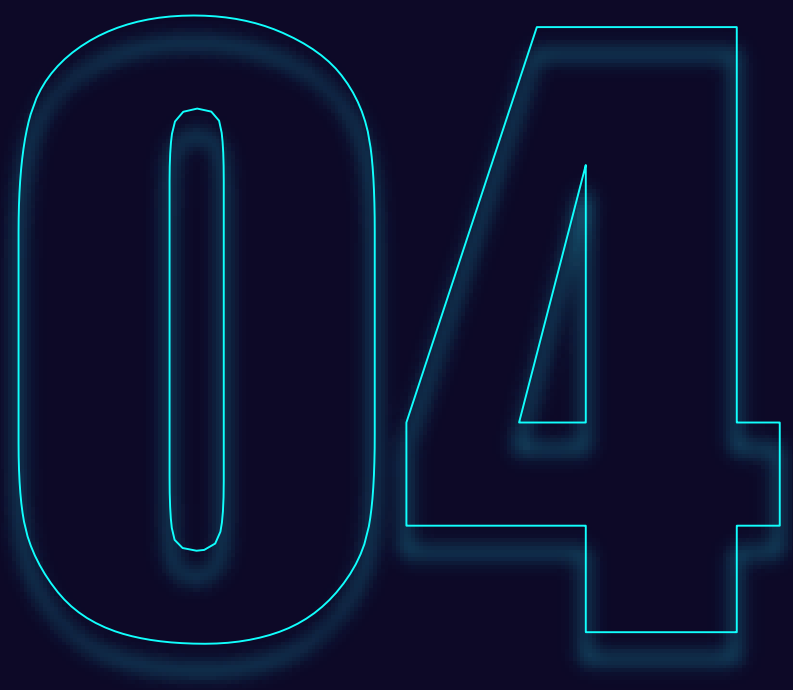
PHISHING: COMO IDENTIFICAR

1. **Rementes Estranhos**
    1. Endereços de e-mail procurados ou que imitam organizações conhecidas (ex.:).**suporte @netflix -supp0rt .com**

2. **E-mails ou Mensagens Urgentes**
    1. Frases como "Atualize sua conta agora" ou "Ação
    2. Pressão para tomar decisões rápidas

3. **Links falsos**
    1. **paypa1.com** e**paypal.com**).
    2. Você

Exemplo real: Joana recebeu um e-mail que parecia ser do banco pedindo confirmação de dados. Ao clicar no link, inseriu suas informações em um site falso, permitindo que hackers acessassem sua conta bancária.



ATUALIZAÇÕES REGULARES

Manter seus sistemas atualizados é vital para a segurança.

ATUALIZAÇÕES REGULARES

Atualizações de software não são apenas para melhorar o desempenho. Elas corrigem vulnerabilidades que cibercriminosos podem explorar. Ignorar essas atualizações pode abrir portas para invasões.

Exemplo real: Carlos, um estudante, teve seu laptop infectado por malware porque ignorou um alerta de atualização que corrigiria uma falha de segurança.

05

FERRAMENTAS DE SEGURANÇA

Ferramentas de segurança podem proteger você contra diversas ameaças digitais

FERRAMENTAS DE SEGURANÇA

Ter um bom software antivírus é essencial para detectar e neutralizar ameaças antes que causem danos. Além disso, firewalls e anti-malware ajudam a criar camadas adicionais de segurança.

Exemplo real: Felipe não usava antivírus e, ao baixar um arquivo suspeito, permitiu que um ransomware criptografasse todos os seus documentos.

REDES WI-FI PÚBLICAS: RISCOS INVISÍVEIS

Redes Wi-Fi públicas, como as de cafeterias ou aeroportos, podem ser perigosas. Hackers podem monitorar o tráfego de dados e capturar informações sensíveis transmitidas sem criptografia.

Exemplo real: Luana, ao usar Wi-Fi público para realizar compras, teve seus dados de cartão de crédito interceptados.

06

O IMPACTO DOS CIBERCRIMES

Esses dados evidenciam a importância de adotar práticas seguras para evitar ser vítima de ataques.

ESTATÍSTICAS E DADOS

O número de ataques cibernéticos cresce cerca de 20% ao ano, tornando a cibersegurança um pilar essencial no mundo digital. Setores como financeiro, saúde, manufatura e governos estão entre os alvos mais visados pelos cibercriminosos, devido ao alto valor das informações que armazenam.

Isso significa não só adotar ferramentas e tecnologias, mas também estruturar processos sólidos de governança, promover capacitação contínua e implementar práticas organizacionais para minimizar vulnerabilidades.

AGRADECIMENTOS

OBRIGADO POR LER ATÉ AQUI

Criei este eBook com a ajuda de uma inteligência artificial e fiz a diagramação manualmente. O guia completo de como desenvolvi está no meu GitHub, caso você queira conferir.

A verdade é que cibersegurança não é mais uma escolha é uma necessidade. Com atitudes simples e o conhecimento certo, você pode evitar perder dinheiro, preservar sua reputação e navegar na internet de forma mais tranquila. Tudo começa agora, e a decisão está nas suas mãos!

https://github.com/Niquefranca