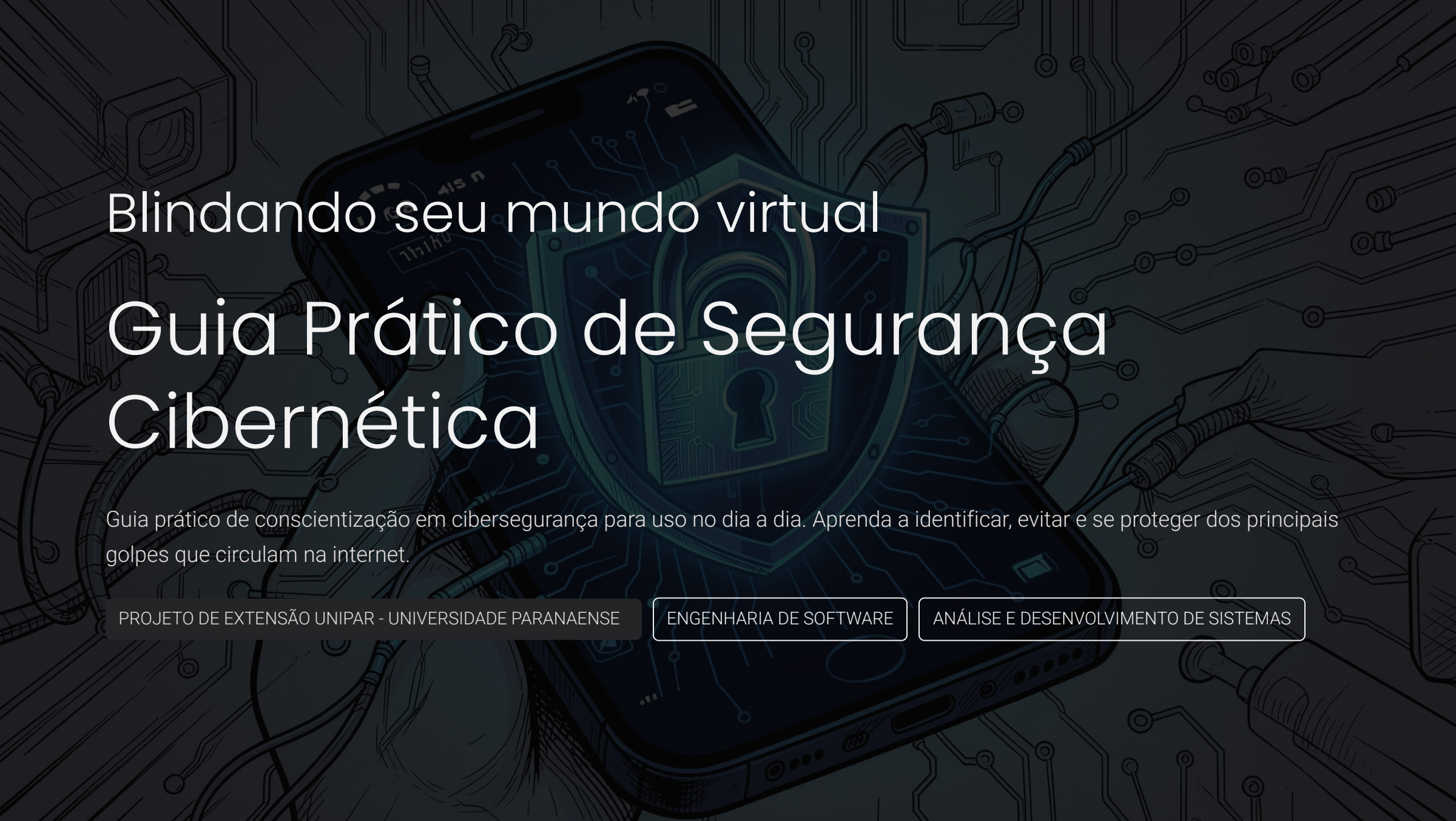


Blindando seu mundo virtual

Guia Prático de Segurança Cibernética

Guia prático de conscientização em cibersegurança para uso no dia a dia. Aprenda a identificar, evitar e se proteger dos principais golpes que circulam na internet.

PROJETO DE EXTENSÃO UNIPAR - UNIVERSIDADE PARANAENSE

ENGENHARIA DE SOFTWARE

ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

Apresentação

A internet trouxe praticidade para nossas vidas. Hoje fazemos pagamentos, compras, estudos e conversamos com pessoas usando apenas o celular. Porém, junto dessa facilidade, cresceram também os **golpes digitais**.

Criminosos utilizam mensagens falsas, redes sociais, aplicativos e até inteligência artificial para enganar pessoas e roubar dinheiro, senhas, dados pessoais, contas bancárias e perfis em redes sociais.

🎯 Ensinar

Como os golpes funcionam e como identificá-los antes que causem danos.

🔍 Alertar

Mostrar os sinais de perigo que muitas pessoas ignoram no dia a dia.

🛡️ Proteger

Explicar como se proteger e adotar hábitos seguros na internet.

⚡ Agir

Ajudar vítimas a agir rapidamente e minimizar os prejuízos causados.

⚠ **Muitas vítimas acreditam que "isso nunca aconteceria comigo."** Mas os golpes atuais são cada vez mais sofisticados e podem atingir qualquer pessoa.

O Que É Cibersegurança?

Cibersegurança é o conjunto de práticas usadas para proteger celulares, computadores, contas online, dados pessoais e informações bancárias. Em palavras simples: é a **"segurança da sua vida digital"**.

Exemplos Práticos

- Criar uma senha forte no Instagram — **isso é cibersegurança.**
- Evitar clicar em links desconhecidos — **isso também é cibersegurança.**
- Ativar a verificação em duas etapas no WhatsApp — **mais um exemplo de proteção digital.**

Privacidade Digital

Privacidade digital significa controlar quem pode acessar seus dados, fotos, conversas, localização e informações pessoais.

Importante: Tudo o que fazemos na internet deixa rastros. Pense antes de compartilhar.

O Crescimento dos Golpes Digitais

Milhões de brasileiros sofrem tentativas de golpe todos os anos. O golpe do Pix cresceu rapidamente após a popularização dos pagamentos instantâneos, e redes sociais e aplicativos de mensagens se tornaram os principais meios usados por criminosos.

Mais Pessoas Conectadas

Hoje praticamente todos utilizam internet diariamente, ampliando o número de vítimas em potencial.

Pagamentos Digitais Rápidos

Transferências acontecem em segundos, facilitando a ação dos criminosos antes que a vítima perceba.

Uso de Inteligência Artificial

Golpistas criam vozes falsas, vídeos manipulados, fotos realistas e mensagens muito convincentes.

Falta de Informação

Muitas vítimas não conhecem os sinais de alerta e caem em golpes que poderiam ser evitados.

> *"Na internet, a pressa é uma das maiores armas dos golpistas."*

Golpe 1 — Phishing: A Pescaria Digital

O que é?

Phishing é um golpe onde criminosos tentam "pescar" informações pessoais da vítima por meio de e-mails falsos, SMS, links suspeitos ou mensagens no WhatsApp.

Como funciona?

A mensagem geralmente diz: *"Sua conta foi bloqueada"*, *"Você ganhou um prêmio"* ou *"Atualize seus dados agora"*.

⚠ **Exemplo real:** "Seu banco detectou atividade suspeita. Clique aqui imediatamente para evitar bloqueio."

🚨 Sinais de Alerta

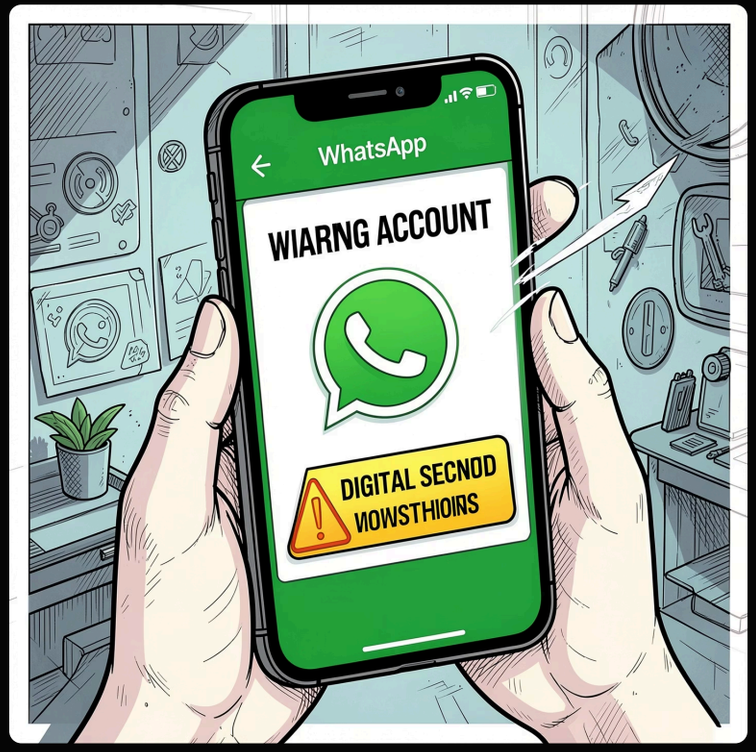
- Urgência exagerada
- Erros de português
- Links estranhos ou encurtados
- Pedido de senha ou dados
- Mensagem alarmante

✅ Como Evitar

- Nunca clique diretamente no link
- Entre pelo aplicativo oficial
- Confira o endereço do site
- Desconfie de mensagens urgentes

Golpe 2 — WhatsApp Clonado

O criminoso tenta roubar o código de verificação da vítima e assume a conta. Depois disso, finge ser a vítima, pede dinheiro para familiares e aplica golpes financeiros.



🚨 Sinais de Alerta

- Código chegando sem você pedir
- Ligações estranhas
- Amigos perguntando sobre pedidos de dinheiro

✅ Como Evitar

- Ative a verificação em duas etapas
- Nunca informe códigos recebidos por SMS
- Proteja seu chip da operadora com senha

Dica de Ouro: Nenhuma empresa séria pede código de verificação por mensagem.

Golpe 3 — Golpe do Pix

Falso Comprovante

O golpista envia um comprovante de Pix falsificado para enganar a vítima.

Pix Agendado

O criminoso agenda uma transferência e cancela antes de ser efetivada.

Pedido Urgente

"Filho, troquei de número. Preciso pagar uma conta urgente." — explore o medo e a pressa.

⚠️ Como Evitar

- Ligue para confirmar a identidade
- Confira nome e CPF antes de transferir
- Desconfie de urgência emocional

🧠 A Psicologia do Golpe

Golpistas exploram **medo, pena e pressão emocional** para fazer a vítima agir sem pensar. Quando você sente urgência, é exatamente o momento de parar e respirar.

Links Falsos, QR Codes e Lojas Online Falsas

🔗 Links e QR Codes Falsos

Criminosos criam sites idênticos aos originais, QR Codes adulterados e páginas falsas de pagamento. Fique atento a URLs estranhas, muitos anúncios e erros visuais.

❌ **bancodobrasil-promocao.net**

✅ **bb.com.br**

🛒 Lojas Online Falsas

Golpistas criam lojas com preços absurdamente baixos, promoções falsas e produtos inexistentes. Desconfie de lojas sem CNPJ, sem avaliações reais e que aceitam apenas Pix.

⚠ **Lembre-se:** "Quando a oferta parece boa demais, desconfie."

✅ Como se Proteger

01

Digite o endereço do site manualmente no navegador

02

Confira o endereço completo antes de inserir dados

03

Evite QR Codes de origem desconhecida

04

Pesquise a reputação da loja e leia reclamações

Engenharia Social, Deepfake e Como se Proteger

🧠 Engenharia Social

Manipulação psicológica para convencer a vítima a entregar informações. O criminoso explora **medo, pressa, autoridade e emoção**.

- "Sou do banco e preciso confirmar seus dados"
- "Seu filho sofreu um acidente"
- "Seu CPF será cancelado"

🤖 Deepfake e IA

Tecnologia que cria vídeos falsos, vozes falsas e imagens manipuladas. Golpistas fingem ser familiares ou simulam voz de empresas para pedir dinheiro.

ⓘ **Como evitar:** Confirme por ligação real, use palavra de segurança familiar e não confie apenas em áudio ou vídeo.

🛡️ Como se Proteger

Senhas Fortes

Misture letras, números e símbolos. Evite datas de nascimento e nomes óbvios.

Autenticação em Dois Fatores

Camada extra de segurança. Mesmo que descubram sua senha, precisarão do código.

Mantenha Tudo Atualizado

Atualizações corrigem falhas de segurança. Atualize celular, navegador e aplicativos.

Cuidado com Wi-Fi Público

Evite acessar banco, fazer compras ou inserir dados pessoais em redes abertas.

Caí em um Golpe. E Agora? + Conclusão

🚨 Passo a Passo se For Vítima

01

Troque suas senhas imediatamente em todas as contas afetadas

02

Avise o banco e bloqueie cartões, Pix e aplicativos bancários

03

Registre boletim de ocorrência — pode ser feito online em muitos estados

04

Avise familiares e contatos para evitar novos golpes usando sua identidade

05

Guarde provas: prints, mensagens, comprovantes e links

✅ Checklist de Segurança Digital

- Uso senhas fortes e únicas
- Tenho verificação em duas etapas
- Desconfio de links e urgências
- Atualizo meus aplicativos
- Confirmo pedidos de dinheiro
- Pesquiso lojas antes de comprar

> **"Na internet, segurança não é exagero. É proteção."**

A melhor defesa contra golpes digitais é **informação, atenção, prevenção e educação digital**. Pequenos cuidados podem evitar perda de dinheiro, roubo de contas e grandes prejuízos emocionais.

PROJETO DE EXTENSÃO UNIVERSITÁRIA | ENGENHARIA DE SOFTWARE