

SEGURANÇA DIGITAL

no Dia a Dia

10 DICAS RÁPIDAS

Para usar a internet com mais segurança



SUPESP-CE

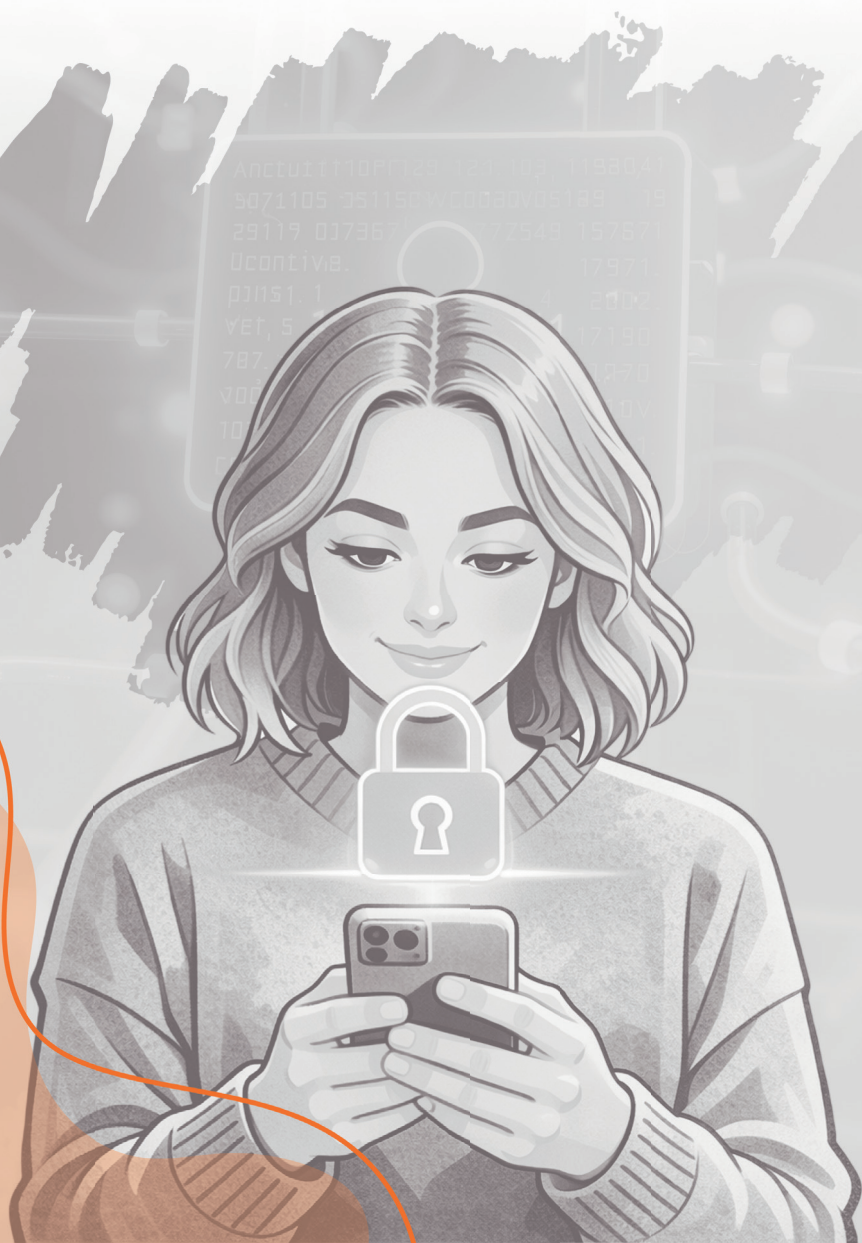
Superintendência de Pesquisa
e Estratégia de Segurança Pública



CEARÁ
GOVERNO DO ESTADO

SECRETARIA DA SEGURANÇA
PÚBLICA E DEFESA SOCIAL

GOVERNO DO ESTADO DO CEARÁ
SECRETARIA DA SEGURANÇA PÚBLICA E DEFESA SOCIAL - SSPDS
SUPERINTENDÊNCIA DE PESQUISA E ESTRATÉGIA DE SEGURANÇA PÚBLICA - SUPESP



GOVERNADOR DO ESTADO DO CEARÁ

Elmano de Freitas da Costa

VICE-GOVERNADORA DO ESTADO DO CEARÁ

Jade Afonso Romero

**SECRETÁRIO DA SEGURANÇA PÚBLICA E DEFESA
SOCIAL - SSPDS**

Antonio Roberto Cesário de Sá

**SUPERINTENDENTE DA SUPERINTENDÊNCIA DE
PESQUISA E ESTRATÉGIA DE SEGURANÇA PÚBLICA**

Juliana Márcia Barroso

**DIRETOR DE PESQUISA E AVALIAÇÃO
DE POLÍTICAS DE SEGURANÇA
PÚBLICA - DIPAS**

José Eudázio Honório Sampaio

**DIRETOR DE ESTRATÉGIA DE
SEGURANÇA PÚBLICA - DIESP**

Gonçalo Eduardo Barreto Araújo

**DIRETOR DE ESTATÍSTICA E
GEOPROCESSAMENTO - DIEST**

Antonio Matheus Osterno Leitão

DIRETORA ADMINISTRATIVO-FINANCEIRO - DIAFI

Leidiane Gomes de Sousa

ELABORAÇÃO TÉCNICA

Estêvão Lima Arrais

DIAGRAMAÇÃO

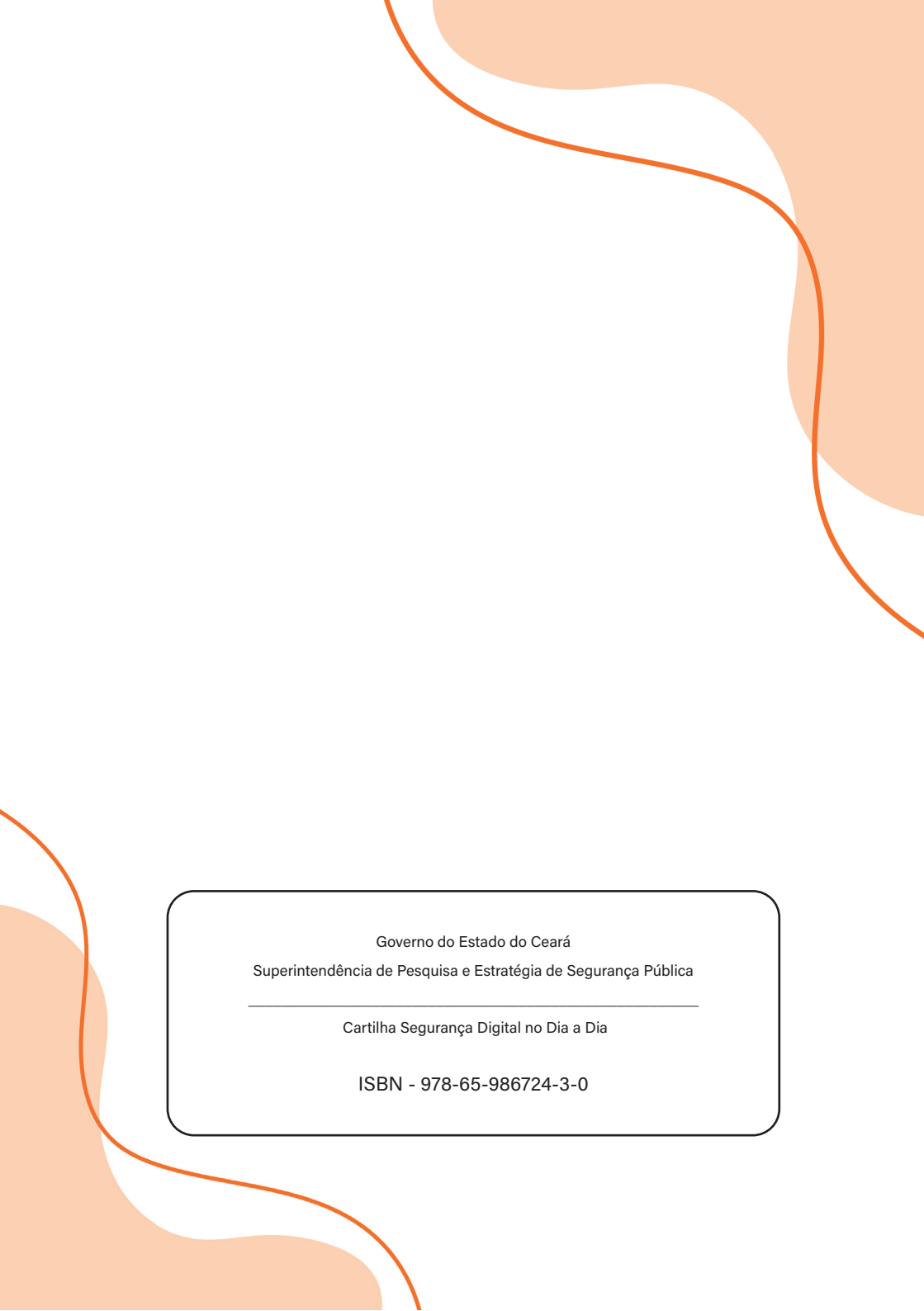
Juliana Mendes Teixeira de Lima



SUPESP-CE
Superintendência de Pesquisa
e Estratégia de Segurança Pública



CEARÁ
GOVERNO DO ESTADO



Governo do Estado do Ceará
Superintendência de Pesquisa e Estratégia de Segurança Pública

Cartilha Segurança Digital no Dia a Dia

ISBN - 978-65-986724-3-0

SUMÁRIO

-  Apresentação
-  1 Golpes financeiros digitais
-  2 Clonagem de contas em aplicativos de mensagens
-  3 Perfis falsos e identidades simuladas
-  4 Roubo e vazamento de dados pessoais
-  5 Links e arquivos maliciosos
-  6 Exposição de Crianças e Adolescentes
-  7 Falsas oportunidades de investimento e promoções
-  8 Exposição excessiva nas redes sociais
-  9 Violências digitais
-  10 Falta de atualização e proteção dos dispositivos
-  Canais de denúncias da Segurança Pública do Ceará

APRESENTAÇÃO

A internet faz parte do cotidiano da maioria das pessoas. Por meio dela, conversamos com familiares e amigos, realizamos pagamentos, acessamos serviços públicos, fazemos compras, estudamos e trabalhamos. Apesar dos benefícios, o ambiente digital também pode trazer riscos, especialmente quando informações pessoais são compartilhadas sem cuidado ou quando desconhecemos as formas mais comuns de golpes e fraudes. Com o propósito de promover a proteção e a conscientização digital da população cearense, a Secretaria da Segurança Pública e Defesa Social do Estado do Ceará (SSPDS/CE), por intermédio da Superintendência de Pesquisa e Estratégia de Segurança Pública (Supesp), apresenta esta cartilha institucional. O material reúne orientações objetivas e diretrizes práticas destinadas a fortalecer o uso seguro, responsável e estratégico das tecnologias digitais no cotidiano.





**FIQUE SEGURO
ONLINE**



ATENÇÃO AO USO DA INTERNET



Use senhas fortes e altere com frequência



Ative a verificação em duas etapas



Desconfie de mensagens suspeitas



Não clique em links duvidosos

1. GOLPES FINANCEIROS DIGITAIS

Fraudes que usam Pix, cartões, falsos atendentes e mensagens falsas se passando por bancos, empresas ou órgãos públicos para roubar dados sensíveis ou forçar transferências indevidas.

EXEMPLO PRÁTICO:

Maria recebeu uma ligação de um “funcionário do banco” alertando sobre uma compra suspeita. Para “cancelar” a operação, ele pediu confirmação de dados ou uma transferência via Pix. Preocupada, Maria seguiu as instruções... e perdeu seu dinheiro.





DICA DE SEGURANÇA



BANCOS E INSTITUIÇÕES PÚBLICAS NUNCA PEDEM:

- Senhas ou códigos de verificação;
- Transferências por telefone, mensagem ou redes sociais.



AO RECEBER UMA COMUNICAÇÃO SUSPEITA:

- Interrompa o contato imediatamente;
- Busque você mesma os canais oficiais (site ou app do banco, telefone conhecido);
- Confirme a informação diretamente, sem usar os dados fornecidos pelo contato suspeito.



ATENÇÃO!

Desconfie, desligue e verifique.

2. CLONAGEM DE CONTAS EM APLICATIVOS DE MENSAGENS

Acesso indevido e clonagem de contas de WhatsApp ou aplicativos similares, utilizados por criminosos para solicitar dinheiro aos contatos da vítima, explorando vínculos de confiança e situações de urgência.

EXEMPLO PRÁTICO:

João recebeu uma mensagem supostamente enviada por sua prima Ana, solicitando dinheiro de forma urgente. Confiando na identidade do remetente, ele realizou a transferência. Posteriormente, constatou que a conta havia sido clonada e que Ana nunca fez o pedido.





DICA DE SEGURANÇA



SEMPRE CONFIRME PEDIDOS DE DINHEIRO POR OUTRO CANAL, MESMO DE CONTATOS CONHECIDOS:

- Ligação telefônica direta;
- Chamada de vídeo;
- Outro meio já confirmado.



ATENÇÃO!

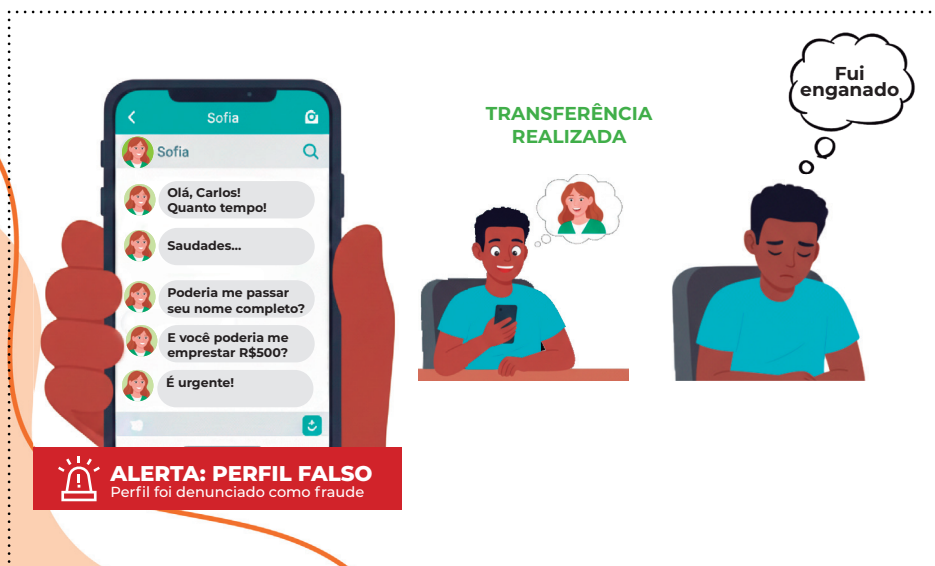
Recebeu pedido de dinheiro? Verifique antes de enviar!

3. PERFIS FALSOS E IDENTIDADES SIMULADAS

Criação de contas falsas ou perfis clonados em redes sociais, utilizados para enganar usuários, obter informações pessoais, estabelecer vínculos de confiança artificiais e aplicar golpes financeiros.

EXEMPLO PRÁTICO:

Carlos aceitou “amizade” de um perfil com nome e foto de uma ex-colega de trabalho. Após conversas, começaram pedidos de dados pessoais e dinheiro. Descoberta: era um perfil falso criado exclusivamente para golpes.





DICA DE SEGURANÇA



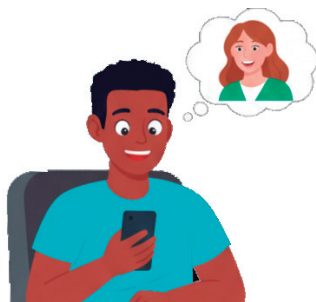
DESCONFIE DE PERFIS COM:

- Poucas fotos ou repetidas;
- Histórico recente (pouco tempo de rede);
- Baixa interação/comentários;
- Pedidos incomuns urgentes ou repetidos.



NA DÚVIDA:

- Ligue ou mande mensagem por outro canal comunicativo;
- Confirme com amigos em comum;
- Denuncie o perfil suspeito à plataforma.



ATENÇÃO!

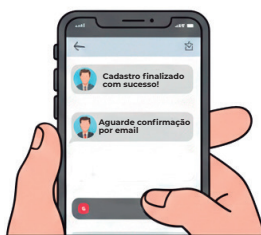
Não compartilhe dados com perfis não verificados!

4. ROUBO E VAZAMENTO DE DADOS PESSOAIS

Uso indevido de CPF, fotos, documentos, senhas e informações bancárias para fins criminosos, como abertura de contas, realização de compras, contratação de serviços ou aplicação de golpes em nome da vítima.

EXEMPLO PRÁTICO:

Paulo enviou, por mensagem, a foto de seu documento para participar de um suposto cadastro online. Dias depois, descobriu que seus dados haviam sido utilizados para abrir contas e realizar compras em seu nome, gerando prejuízos financeiros e transtornos legais.



ALERTA: VAZAMENTO DE DADOS

Seus dados foram utilizados para abertura de contas não autorizadas e compras online



DICA DE SEGURANÇA



NUNCA COMPARTILHE DADOS POR:

- Mensagens (WhatsApp, redes sociais);
- Sites desconhecidos ou não oficiais;
- E-mails suspeitos;
- Ligações de números desconhecidos.



COMO PROTEGER SEUS DADOS:

- Forneça informações apenas em canais oficiais (mas sempre verifique o endereço URL);
- Fontes previamente confirmadas;
- Ambientes seguros e necessários.



ATENÇÃO!

Só compartilhe quando essencial e com fonte verificada!

5. LINKS E ARQUIVOS MALICIOSOS

Mensagens que contêm links maliciosos, capazes de direcionar a páginas falsas ou instalar vírus e programas espiões em celulares e computadores, permitindo o acesso não autorizado a dados e contas da vítima.

EXEMPLO PRÁTICO:

Fernanda recebeu uma mensagem informando que havia ganhado um prêmio e foi incentivada a clicar em um link. Após o acesso, seu celular passou a apresentar falhas e, em seguida, foram identificados acessos não autorizados às suas contas, caracterizando a infecção por software malicioso.





DICA DE SEGURANÇA



NÃO CLIQUE EM LINKS QUE:

- Chegam inesperadamente por mensagem;
- Prometem prêmios, descontos ou vantagens “imperdíveis”;
- São enviados por remetentes desconhecidos;
- Geram sensação de urgência ou curiosidade.



COMO AGIR:

- Não clique e apague a mensagem.



ATENÇÃO!

Desconfie e delete: acesse apenas links confiáveis.

6. EXPOSIÇÃO DE CRIANÇAS E ADOLESCENTES

Manipulação psicológica que explora emoções, empatia e senso de urgência para induzir comportamentos de risco, incluindo a exposição indevida e a adultização de crianças e adolescentes em ambientes digitais com objetivos de engajamento, monetização ou obtenção de vantagens financeiras.

EXEMPLO PRÁTICO:

Um responsável cria e publica vídeos de crianças/adolescentes em situações constrangedoras ou emocionalmente sensíveis. Ele busca induzir comportamentos que estimulem comentários, doações e visualizações lucrativas.





DICA DE SEGURANÇA



NÃO PARTICIPE:

- Não compartilhe, curta ou comente;
- Não contribua financeiramente;
- Não normalize conteúdos que exponham menores de idade, sexualização de crianças e adolescentes e que usam vulnerabilidade para engajamento.



SEU PAPEL É PROTEGER:

- Ao identificar conteúdo suspeito, denuncie na própria plataforma, registre no Conselho Tutelar da sua cidade;
- Comunique órgãos competentes (Polícia e Ministério Público);
- Ative o controle parental nas redes sociais para monitorar o tempo de uso e restringir o acesso a conteúdos inadequados para crianças e adolescentes.



ATENÇÃO!

A imagem e o desenvolvimento saudável de crianças e adolescentes vêm antes de qualquer engajamento ou monetização digital.

7. FALSAS OPORTUNIDADES DE INVESTIMENTO E PROMOÇÕES

Anúncios ou mensagens enganosas que prometem ganhos rápidos, descontos irreais ou prêmios inexistentes, explorando a expectativa de lucro fácil para induzir a vítima a transferências financeiras ou ao fornecimento de dados pessoais.

EXEMPLO PRÁTICO:

Ricardo visualizou um anúncio nas redes sociais prometendo altos ganhos por meio de um investimento “sem risco” e com retorno imediato. Após realizar a transferência do valor solicitado, o perfil ou contato desapareceu, caracterizando a fraude.





DICA DE SEGURANÇA



SINAIS DE ALERTA

- Desconfie de ofertas que garantem lucro rápido/fácil e prometem retorno sem risco;
- Anúncios que criam sensação de urgência.



PROTEÇÃO ANTES DE INVESTIR:

- Busque informações em fontes confiáveis;
- Verifique a credibilidade da empresa/fornecedor;
- Consulte órgãos reguladores (CVM, Banco Central);
- Evite decisões impulsivas: ganho fácil não existe!



ATENÇÃO!

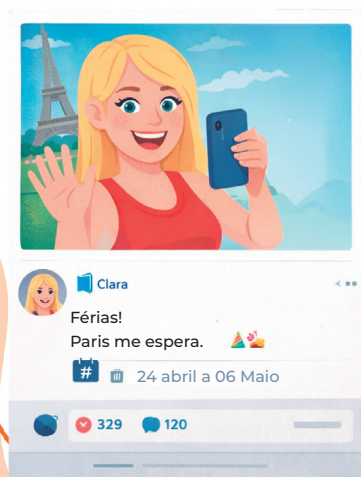
Dinheiro fácil? Investimento certo? Desconfie: é golpe!

8. EXPOSIÇÃO EXCESSIVA NAS REDES SOCIAIS

Compartilhamento excessivo de rotina, localização, viagens e informações pessoais em redes sociais, prática que facilita a atuação de criminosos e a aplicação de golpes, além de expor a vítima a outros riscos.

EXEMPLO PRÁTICO:

Clara publicou nas redes sociais que estaria viajando por vários dias, indicando locais e períodos de ausência. Durante esse intervalo, criminosos utilizaram essas informações para tentar aplicar golpes em seu nome e planejar outras ações ilícitas.





DICA DE SEGURANÇA



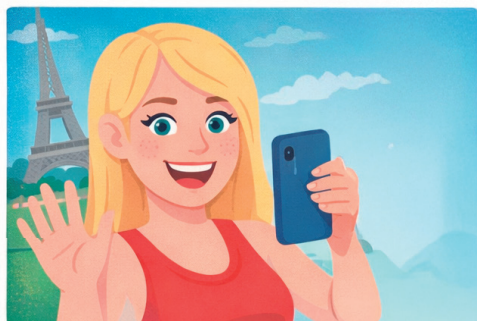
EVITE DIVULGAR:

- Localização em tempo real (check-ins, geolocalização);
- Datas exatas de viagem;
- Fotos que mostram endereço, documentos ou rotina fixa.



MELHORES PRÁTICAS:

- Compartilhe apenas com círculo de amigos e familiares de restrita confiança;
- Nunca compartilhe várias informações combinadas (ex: foto da casa + endereço + datas e bilhete de viagem).



ATENÇÃO!

O que você publica pode ser visto por quem você não conhece.

9. VIOLÊNCIAS DIGITAIS

Práticas de violência digital que incluem ofensas, ameaças, perseguição online, webbullying e a divulgação indevida de imagens ou informações pessoais, com potencial de causar danos emocionais, psicológicos e sociais à vítima.

EXEMPLO PRÁTICO:

Lucas passou a receber mensagens ofensivas e ameaças constantes em redes sociais, muitas delas públicas, o que lhe causou sofrimento, insegurança e receio de se expor no ambiente digital.





DICA DE SEGURANÇA



NÃO FAÇA:

- Não responda às ofensas;
- Não minimize a situação.



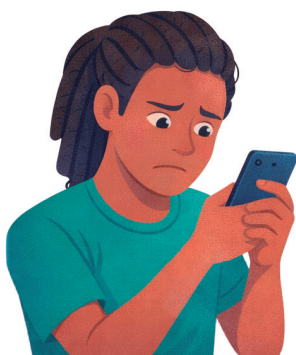
AÇÕES IMEDIATAS DE PROTEÇÃO:

- Bloqueie o agressor;
- Preserve as provas (prints, links, datas e horários);
- Denuncie o perfil/comentário na plataforma;
- Busque apoio emocional (família, amigos e profissionais).

CASOS GRAVES OU REINCIDENTES:

Registre ocorrência policial para:

- Ameaças;
- Perseguição (stalking);
- Humilhação ou intimidação (webbullying);
- Divulgação não consensual de imagens íntimas;
- Discriminação ou incitação à violência.



ATENÇÃO!

Violência digital é crime. Você não está sozinho(a).
Denuncie e preserve sua saúde digital.

10. FALTA DE ATUALIZAÇÃO E PROTEÇÃO DOS DISPOSITIVOS

Uso de celulares, computadores e outros dispositivos digitais sem atualizações de segurança, sem antivírus ou sem mecanismos básicos de proteção, o que aumenta significativamente a vulnerabilidade a acessos indevidos.

EXEMPLO PRÁTICO:

O celular de Letícia não possuía bloqueio de tela nem estava atualizado. Após a perda do aparelho, terceiros conseguiram acessar aplicativos bancários e redes sociais, ocasionando prejuízos financeiros e uso indevido de suas informações.





DICA DE SEGURANÇA



BLOQUEIO DE ACESSO E ATUALIZAÇÕES CONSTANTES:

- Sempre opte por senhas fortes (letras maiúsculas e minúsculas, números e caracteres especiais) e biometria (impressão digital);
- Certifique de atualizar constantemente o sistema operacional do seu celular e aplicativos (especialmente bancários);
- Cadastre seu celular no programa estadual “Meu Celular”.
Link do Programa: <https://meucelular.sspds.ce.gov.br/>



ATENÇÃO!

Poucos minutos de configuração evitam grandes prejuízos.

SEGURANÇA DIGITAL

TODOS PODEM CONTRIBUIR

A proteção online se constrói no dia a dia com:

Atenção aos sinais de risco;

Informação sobre os golpes mais comuns;

Hábitos simples de prevenção.





CUIDADOS QUE FAZEM A DIFERENÇA:



Verifique antes de clicar ou transferir



Proteja seus dispositivos e dados



Pense antes de compartilhar



Desconfie de oportunidades “perfeitas”

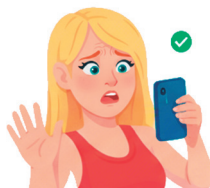


Denuncie conteúdos e comportamentos abusivos

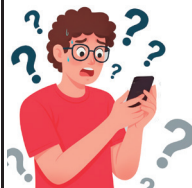
ESSAS PRÁTICAS PREVINEM:



Prejuízos
financeiros



Danos
à imagem
e reputação



Sofrimento
emocional



Exposição
indevida de
terceiros

**TODOS PODEM COLABORAR PARA UM
AMBIENTE ONLINE, SEGURO E CONSCIENTE**

CANAIS DE DENÚNCIAS DA SEGURANÇA PÚBLICA DO CEARÁ

A SSPDS-CE disponibiliza canais específicos para denúncias, incluindo crimes de segurança digital, garantindo total anonimato.

SERVIÇO ONLINE DE DENÚNCIAS



Não é necessário se identificar.



Telefone:
181



WhatsApp:
(85) 3101-0181



Canal online
Complementar



<https://disquedenuncia181.sspds.ce.gov.br>

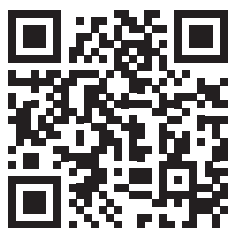


CADASTRE-SE E FACILITE A RECUPERAÇÃO DO SEU CELULAR EM CASO DE PERDA, ROUBO OU FURTO

O sistema “Meu Celular”, desenvolvido pela Coordenação de Tecnologia da Informação e Comunicação (Cotic) da SSPDS/CE, permite que usuários cadastrem seus aparelhos com dados pessoais para, em caso de roubo ou furto, notificarem rapidamente as autoridades policiais, visando aumentar a recuperação dos dispositivos e reduzir esse tipo de crime no estado.

1. Cadastre seu celular a qualquer momento.(<https://meucelular.sspds.ce.gov.br/>)
2. Em caso de perda, roubo ou furto, você pode criar um pré-alerta.
3. Após fazer e incluir o Boletim de Ocorrência, o alerta será criado para a polícia.
4. Pronto, as forças de segurança entram em ação para recuperar seu celular.





SUPESP-CE
Superintendência de Pesquisa
e Estratégia de Segurança Pública



CEARÁ
GOVERNO DO ESTADO