

SEGURANÇA DIGITAL

nas Redes Sociais

10 DICAS RÁPIDAS

Para usar a internet com mais segurança

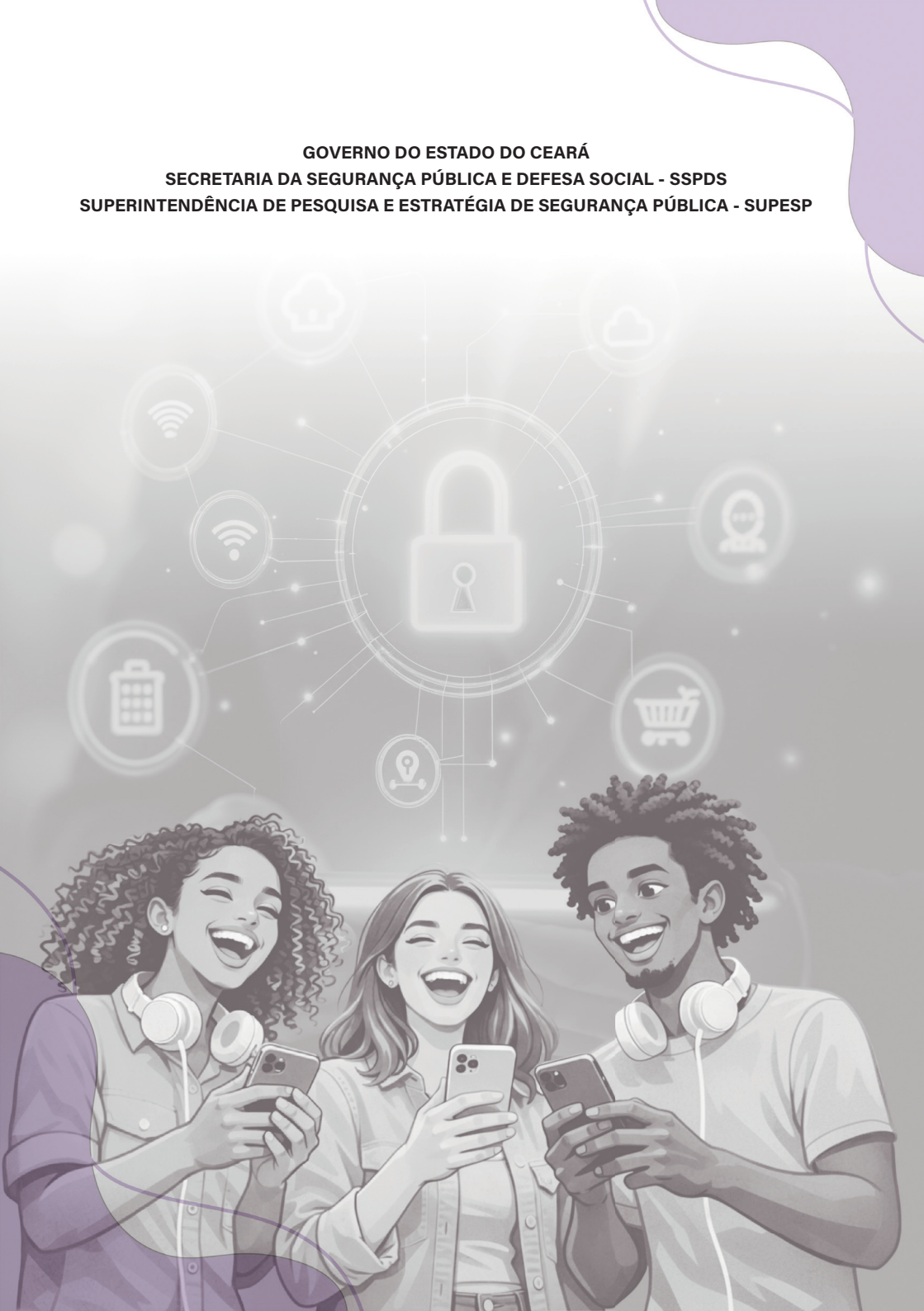


SUPESP-CE
Superintendência de Pesquisa
e Estratégia de Segurança Pública



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 nas Redes Sociais
ISBN - 978-65-986724-4-7

SUMÁRIO

-  Apresentação
-  1 Desconfie de pedidos urgentes de dinheiro, pagamentos e transferências
-  2 Nunca compartilhe senhas ou códigos
-  3 Evite clicar em links suspeitos
-  4 Verifique perfis antes de interagir
-  5 Cuidado com ofertas e investimentos fáceis
-  6 Controle o que você compartilha
-  7 Use senhas fortes e diferentes
-  8 Ativar a segurança nas redes sociais
-  9 Bloqueie e denuncie comportamentos abusivos
-  10 Proteja crianças e adolescentes nas redes sociais
-  Canais de denúncias da Segurança Pública do Ceará

APRESENTAÇÃO

As redes sociais fazem parte do dia a dia de milhões de pessoas. Plataformas como WhatsApp, Instagram, X, TikTok e Facebook facilitam a comunicação, o acesso à informação e os negócios. No entanto, também podem ser usadas para golpes, fraudes e outras situações de risco. Adotar cuidados simples ajuda a proteger sua conta, seus dados e suas relações. 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.



ATENÇÃO AO USO DA INTERNET



**FIQUE SEGURO
ONLINE**

Proteja-se nas redes sociais!



**Proteja
sua conta**

Use senhas fortes
e autenticação em
duas etapas.



**Fique
atento
a golpe**

Cuidado com
mensagens
urgentes pedindo
dinheiro.



**Desconfie
de links e
sites**

Sempre confira a
URL das páginas
e evite clicar em
links suspeitos.



**Acesse
sempre
canais
oficiais**

Em caso de dúvida,
entre em contato
com o suporte dos
canais oficiais.

***Adote cuidados simples para evitar golpes e
proteger sua privacidade!***

1. DESCONFIE DE PEDIDOS URGENTES DE DINHEIRO, PAGAMENTOS E TRANSFERÊNCIAS

Mensagens fraudulentas que exploram urgência, medo ou confiança para solicitar transferências imediatas, geralmente usando contas clonadas ou se passando por pessoas próximas.

EXEMPLO PRÁTICO:

Carlos recebeu uma mensagem falsa no “ZapNote”, supostamente de um familiar, pedindo dinheiro com urgência devido a uma emergência. Alarmado, ele fez a transferência, mas depois descobriu que a conta havia sido clonada e o pedido era uma fraude.





DICA DE SEGURANÇA



PARE, PENSE E CONFIRME ANTES DE AGIR:

- Golpes exploram urgência para impedir seu raciocínio;
- Desconfie de pedidos “só por esta vez” ou “não conte para ninguém”.



ANTES DE QUALQUER TRANSFERÊNCIA:

- Ligue diretamente para a pessoa;
- Faça uma videochamada para ver e ouvir quem está falando;
- Pergunte detalhes que só ela sabe.



ATENÇÃO!

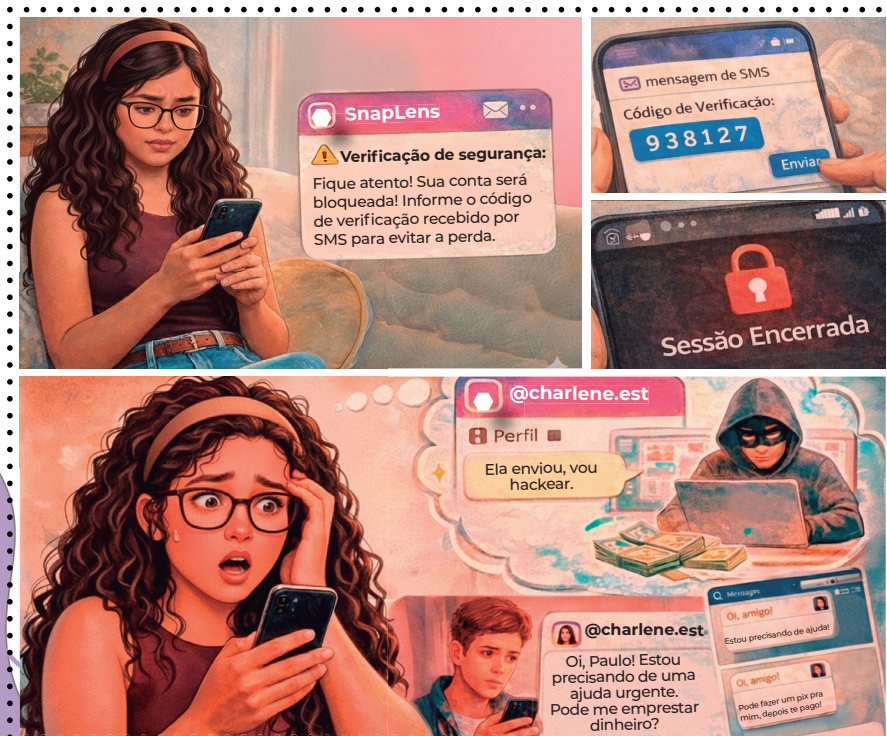
Uma ligação de confirmação pode evitar um grande prejuízo.

2. NUNCA COMPARTILHE SENHAS OU CÓDIGOS

Tentativas de obtenção indevida de senhas, códigos de verificação ou autenticação em duas etapas, utilizadas para invadir contas, assumir perfis e aplicar golpes em nome da vítima.

EXEMPLO PRÁTICO:

Charlene recebeu no “SnapLens” uma mensagem falsa pedindo que “verificasse” sua conta enviando um código SMS. Ao repassar o código, perdeu o controle do perfil, que foi usado pelo criminoso para enviar mensagens fraudulentas aos seus contatos.





DICA DE SEGURANÇA



EM CASO DE SUSPEITA:

- Interrompa o contato imediatamente;
- Não responda e não compartilhe nenhuma informação;
- Use apenas os canais oficiais da plataforma para verificação.



REGRAS DE OURO:

- Senhas e códigos são pessoais e intransferíveis;
- Desconfie de qualquer pedido de senha ou código. Nenhuma instituição solicita esse tipo de informação.



ATENÇÃO!

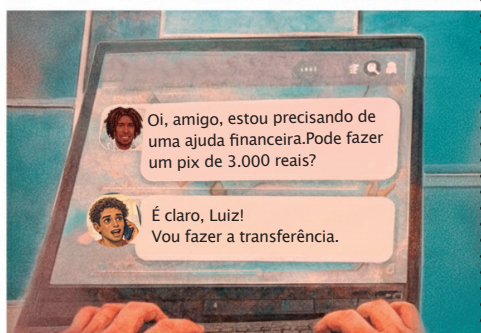
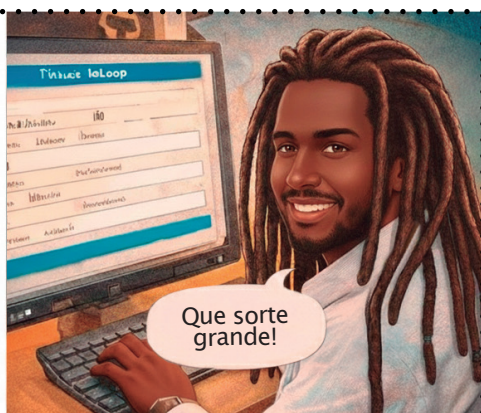
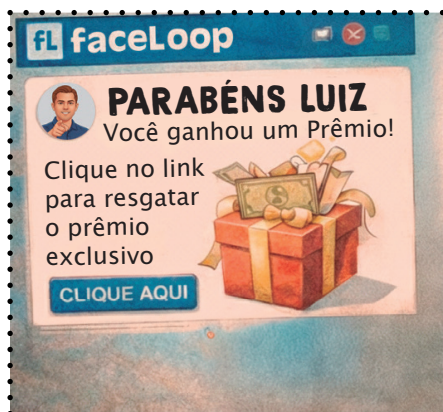
Sua senha é como a chave da sua casa digital. Quem tem acesso a ela pode entrar na sua conta.

3. EVITE CLICAR EM LINKS SUSPEITOS

Links maliciosos enviados por mensagens, comentários ou publicações em redes sociais, que direcionam a páginas falsas criadas para capturar dados pessoais, senhas ou instalar programas maliciosos.

EXEMPLO PRÁTICO:

Luiz recebeu no FaceLoop um link falso anunciando que ele havia ganhado um prêmio. Ao inserir seus dados na página, teve sua conta comprometida, resultando em acessos indevidos e uso fraudulento do perfil.





DICA DE SEGURANÇA



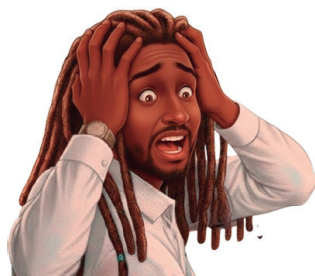
SINAIS DE ALERTA:

- Não clique em links recebidos inesperadamente;
- Desconfie de ofertas “boas demais para ser verdade” (prêmios, descontos irreais);
- Verifique a origem da mensagem.



PROCEDIMENTOS SEGUROS:

- Digite manualmente o endereço oficial no navegador;
- Acesse diretamente o site da empresa/instituição;
- Verifique a informação por canais oficiais.



ATENÇÃO!

Um clique pode colocar sua conta em risco.

4. VERIFIQUE PERFIS ANTES DE INTERAGIR

Perfis falsos ou clonados em redes sociais, criados para se passar por pessoas reais, com o objetivo de enganar usuários, obter informações, aplicar golpes ou induzir comportamentos de risco.

EXEMPLO PRÁTICO:

Roberta aceitou uma solicitação de amizade no FaceLoop de um perfil falso que usava a foto e o nome de alguém conhecido. Após isso, recebeu mensagens suspeitas e descobriu que o perfil foi criado para enganar seus contatos.





DICA DE SEGURANÇA



SINAIS DE ALERTA:

- Perfil recém-criado e pouca ou nenhuma interação;
- Fotos repetidas ou de baixa qualidade;
- Pedidos incomuns logo após aceitar.



SINAIS DE CONFIABILIDADE:

- Perfil antigo (criado há meses/anos);
- Amigos em comum consistentes;
- Histórico de publicações regular e real;
- Interações autênticas (comentários e reações).



ATENÇÃO!

Nem todo perfil com foto conhecida é verdadeiro.

5. CUIDADO COM OFERTAS E INVESTIMENTOS FÁCEIS

Golpes baseados em promessas de lucro rápido, prêmios ou descontos irreais, que exploram a expectativa de ganho fácil para induzir a vítima a transferências financeiras ou ao fornecimento de dados pessoais.

EXEMPLO PRÁTICO:

Tiago viu no SnapLens um anúncio com um produto muito abaixo do preço de mercado, fez a transferência solicitada, mas o perfil foi excluído logo depois, impossibilitando contato e configurando uma fraude.





DICA DE SEGURANÇA



ANTES DE QUALQUER PAGAMENTO:

- Pesquise a empresa/ vendedor em fontes confiáveis;
- Verifique a idoneidade da oferta;
- Consulte sites de reclamações (Reclame Aqui, Procon);
- Busque referências de outros compradores.



SINAIS DE ALERTA:

- Ganhos garantidos sem risco;
- Retorno imediato prometido;
- Pressão para decisão rápida;
- Preços absurdamente baixos.



ATENÇÃO!

Pesquise, confirme e decida com segurança.

6. CONTROLE O QUE VOCÊ COMPARTILHA

Exposição excessiva de rotina, localização e informações pessoais em redes sociais, que pode ser utilizada por terceiros para aplicar golpes, fraudes ou outras práticas criminosas.

EXEMPLO PRÁTICO:

Janaina compartilhou detalhes de sua viagem e rotina no SnapLens, incluindo horários e locais. Posteriormente, identificou tentativas de golpe e abordagens suspeitas que usavam as informações de suas publicações, expondo-se a riscos de segurança.





DICA DE SEGURANÇA



EVITE COMPARTILHAR:

- Datas exatas de viagem;
- Endereço residencial ou trabalho;
- Documentos pessoais (RG, CPF, cartões);
- Rotinas diárias previsíveis;
- Fotos que revelem localização específica.



PRÁTICAS SEGURAS:

- Compartilhe viagens APÓS o retorno;
- Desative geolocalização em tempo real;
- Não divulgue horários e rotinas fixas;
- Restrinja visualização a contatos de confiança.



ATENÇÃO!

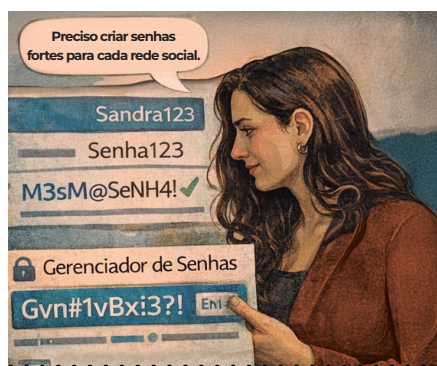
Sua privacidade digital vale mais que likes.
Pense antes de postar.

7. USE SENHAS FORTES E DIFERENTES

Uso da mesma senha em diferentes redes sociais e serviços digitais, prática que amplia significativamente o risco de invasões em cadeia quando uma única conta é comprometida.

EXEMPLO PRÁTICO:

Sandra usava a mesma senha no SnapLens e no FaceLoop. Quando uma das contas foi invadida, os criminosos acessaram automaticamente as demais, ampliando os danos e o alcance do golpe.





DICA DE SEGURANÇA



SINAIS DE ALERTA

- Sequências óbvias: 123456, abcdef;
- Dados pessoais: nome, data nascimento, CPF;
- Palavras comuns: senha, password, admin;
- Substituições previsíveis: “@” por “a”, “l” por “i”.



CRITÉRIOS PARA SENHAS FORTES:

- Mínimo 12 caracteres;
- Combine: Letras maiúsculas + minúsculas + números + símbolos;



ATENÇÃO!

Uma senha forte é sua primeira linha de defesa. Diversificar é tão importante quanto fortalecer.

8. ATIVAR A SEGURANÇA NAS REDES SOCIAIS

Ausência de recursos adicionais de proteção, como a verificação em duas etapas, que amplia a vulnerabilidade das contas digitais e facilita invasões e usos indevidos.

EXEMPLO PRÁTICO:

Anna Júlia teve seu ZapNote invadido, e criminosos enviaram mensagens pedindo dinheiro a seus contatos. No entanto, como ela havia ativado a verificação em duas etapas, conseguiu recuperar a conta rapidamente e impedir acessos futuros, limitando os danos.





DICA DE SEGURANÇA



RECURSOS ESSENCIAIS PARA ATIVAR:

- Verificação em duas etapas;
- Aplicativos Autenticadores;
- Alertas de segurança.



CHECKLIST DE PROTEÇÃO:

- 2FA ativado em todas as contas principais;
- E-mail de recuperação atualizado e seguro;
- Número de telefone vinculado e atual.



ATENÇÃO!

Com verificação em duas etapas, sua conta fica mais protegida contra invasores.

9. BLOQUEIE E DENUNCIE COMPORTAMENTOS ABUSIVOS

Ofensas, ameaças, intimidações e perseguições praticadas por meio de redes sociais e aplicativos de mensagens, com potencial de causar danos emocionais, constrangimento, medo e impacto à vida pessoal da vítima.

EXEMPLO PRÁTICO:

Rodrigo começou a receber comentários ofensivos e mensagens agressivas de forma recorrente no SnapLens, com ataques direcionados à sua imagem pessoal. A situação causou desconforto, constrangimento e uma sensação de insegurança ao usar a plataforma.





DICA DE SEGURANÇA



AÇÃO IMEDIATA RECOMENDADA:

- Bloqueie o agressor em todas as plataformas;
- Evite qualquer resposta ou confronto direto;
- Salve as mensagens e registros antes de bloquear e denunciar;
- Registre ocorrência policial para casos recorrentes;
- Acompanhe o status da denúncia.



ATENÇÃO!

Violência digital é crime. Seu silêncio só favorece o agressor. Denuncie, bloqueie e busque apoio.

10. PROTEJA CRIANÇAS E ADOLESCENTES NAS REDES SOCIAIS

Riscos associados à exposição de crianças e adolescentes em redes sociais, como aliciamento, exploração sexual, cyberbullying, desafios perigosos, discurso de ódio e contato com adultos mal-intencionados.

EXEMPLO PRÁTICO:

Afonso faz amizade em um jogo on-line e é convencido a conversar no GameTalk. O jogador tenta ganhar sua confiança e pede uma foto pessoal em troca de vantagens no jogo, exigindo segredo. Com a orientação de um adulto, Afonso reconhece o risco, bloqueia o contato e denuncia a situação.





DICA DE SEGURANÇA



AÇÕES PREVENTIVAS PARA RESPONSÁVEIS:

- Converse sobre os riscos reais da internet, ensine a identificar comportamentos suspeito;
- Mantenha canal aberto para relatos de situações desconfortáveis;
- Conheça as plataformas, monitore listas de amigos e seguidores,acompanhe o histórico de atividades e use ferramentas de controle parental.



ATENÇÃO!

Proteção digital é parte da educação. Um adulto atento pode prevenir danos irreparáveis na vida de uma criança ou adolescente.



SEGURANÇA DIGITAL: UM COMPROMISSO DIÁRIO



A BASE DA PROTEÇÃO ONLINE:

Atenção aos detalhes e sinais suspeitos

Mantenha-se atualizado sobre riscos e golpe

Cultive hábitos conscientes em cada interação



O RESULTADO DOS PEQUENOS CUIDADOS:

Evita prejuízos financeiros

Protege sua privacidade e imagem

Garante experiências digitais mais seguras



**Cada pessoa informada
é uma barreira a mais
contra golpes**



PARA NÃO ESQUECER:



SEU PERFIL É SUA IDENTIDADE DIGITAL



SEU CUIDADO É SUA MAIOR PROTEÇÃO



SUA SENHA É SUA CHAVE PESSOAL

#Use com segurança
#Compartilhe proteção



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>

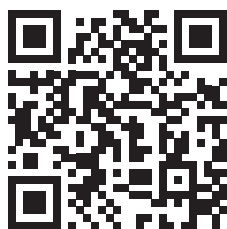


CADASTRE-SE E FACILITE A RECUPERAÇÃO DO SEU CELULAR EM CASO DE PERDA, ROUBO OU FURTO

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