NAVEGANDO SEGURO

ACESSANDO A REDE COM RESPONSABILIDADE

PREFEITURA DE CAÇADOR

Cuidar do presente, transformar o futuro!

SECRETARIA DE EDUCAÇÃO

PREFEITURA MUNICIPAL DE CAÇADOR
SECRETARIA DE EDUCAÇÃO

Alencar Mendes
Prefeito Municipal de Caçador

Manoel de Padua Paiva Moraes
Secretário de Educação

Cleide Alves
Secretária Adjunta de Educação

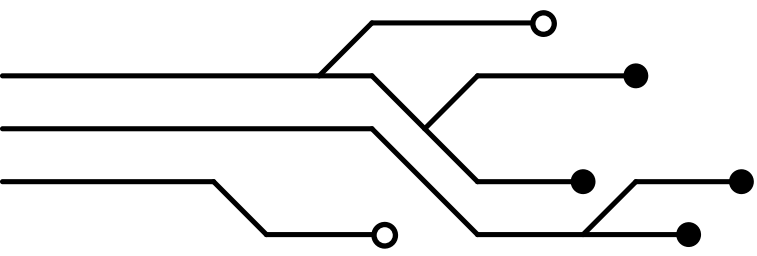
Fabiane Constantini
Coordenadora de Assuntos Administrativos Pedagógicos

Alexandre Maicon de Lima
Coordenador de Tecnologia da Informação

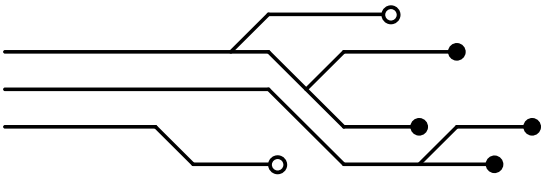
Jean Lucas Tavares
Coordenador Pedagógico de Informática

Gabriel Dalcortivo
LabTec Móvel

Talles Carvalho Elizei
Professor de Informática



SUMÁRIO



Introdução

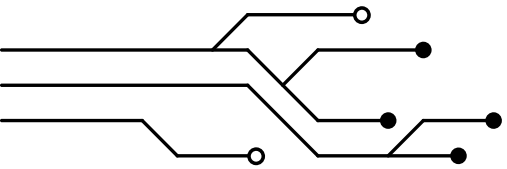
Olá!

É uma alegria poder compartilhar com você esta cartilha feita com muito cuidado pela equipe da Secretaria Municipal de Educação de Caçador. Aqui, reunimos dicas e informações valiosas para que você possa usar a internet de forma mais segura e consciente, seja na escola, em casa ou em qualquer outro lugar.

O mundo digital faz parte do nosso dia a dia, mas é importante lembrar que, assim como nas ruas, também precisamos nos proteger enquanto navegamos por sites, redes sociais e aplicativos. Nesta cartilha, vamos falar sobre temas como senhas seguras, cyberbullying, privacidade, desinformação, entre outros assuntos que ajudam você a se cuidar e a cuidar dos outros também.

Tudo isso é apresentado de forma simples e com uma linguagem acessível, porque aprender sobre segurança digital pode e deve ser algo simples.

Boa leitura.



Criação e Gerenciamento de Senhas

As senhas são como chaves digitais: elas protegem nossas informações pessoais, redes sociais, mensagens e até contas bancárias. Por isso, criar e cuidar bem das suas senhas é essencial para manter sua segurança na internet.

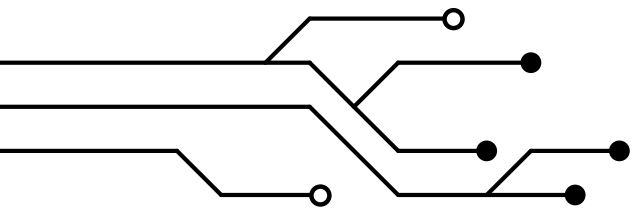
Como criar uma senha segura?

Uma **senha forte** deve ser:

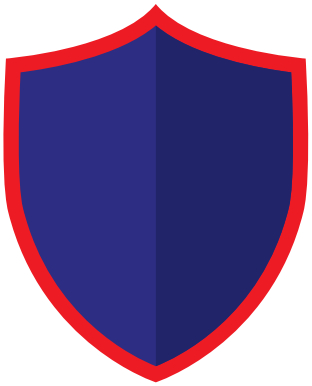
- **Única: não use a mesma senha para tudo.**
- **Longa: quanto maior, melhor! Tente usar pelo menos 12 caracteres.**
- **Imprevisível: evite datas de nascimento, nomes de familiares ou combinações como "123456", "senha", "qwerty".**

O que não fazer?

- **Usar a mesma senha para várias contas.**
- **Compartilhar senhas com outras pessoas (mesmo amigos próximos).**
- **Anotar senhas em papéis deixados em locais visíveis.**
- **Salvar senhas no navegador de forma automática sem proteção.**



Criação e Gerenciamento de Senhas



Dica de como ter uma senha segura:

- Use uma frase longa com variações, por exemplo:

"CachorroDoLucas@2025CorreMuito!“

- Ative a Autenticação de Dois Fatores, pois, mesmo que alguém descubra sua senha, ainda precisará de um segundo código para acessar sua conta.

LEMBRE-SE!

Senhas são segredos pessoais que ajudam a proteger tudo o que fazemos online. Busque sempre criar senhas criativas e ajude os mais novos a memorizá-las de forma divertida (como usando uma rima ou imagem mental).

Cuidados com Informações Pessoais

Na internet, nossas informações podem dizer muito sobre nós e isso pode ser usado por pessoas mal-intencionadas se cair nas mãos erradas. Por isso, é muito importante saber o que e com quem compartilhamos nossos dados.

O que são dados pessoais?

Alguns exemplos:

- Nome completo
- Idade e data de nascimento
- Endereço e nome da escola
- Número de telefone
- CPF e RG
- Fotos e vídeos
- Localização em tempo real

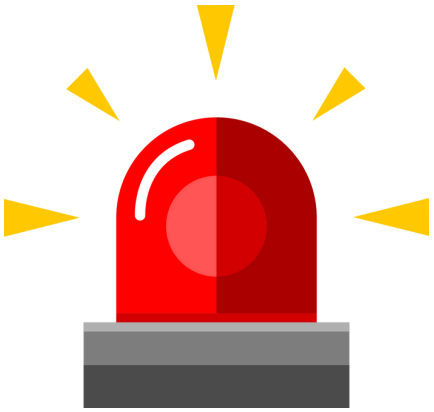
Quando é seguro compartilhar?

Compartilhe informações pessoais apenas quando for necessário e com pessoas ou instituições de confiança. Em redes sociais, evite:

- Nome completo
- Idade e data de nascimento
- Endereço e nome da escola
- Número de telefone
- CPF e RG
- Fotos e vídeos
- Localização em tempo real

Cuidados com Informações Pessoais

ALERTA!



Na internet, existem muitas armadilhas criadas para enganar as pessoas e roubar informações.

Fique de olho em sinais de alerta!

Sinais de que algo pode ser um golpe:

- Mensagens dizendo que você ganhou um prêmio, sorteio ou dinheiro (mesmo sem ter participado de nada);
- Pedidos de dados pessoais ou senhas por e-mail, mensagem ou redes sociais;
- Alguém dizendo que é de um banco ou empresa e pedindo que você "confirme" informações;
- Pessoas desconhecidas pedindo dinheiro ou fazendo chantagens com fotos e informações.

Importante: bancos, escolas, empresas sérias nunca pedem informações sensíveis por WhatsApp ou redes sociais.

Cuidados com Informações Pessoais

O que fazer quando achar algo suspeito?

- Não clique em links de origem duvidosa.
- Converse com um adulto de confiança ou responsável (se for aluno).
- Bloqueie e denuncie o número ou perfil.
- Tire print da mensagem e, se for o caso, registre um boletim de ocorrência.

O que fazer quando eu cair em um golpe?

Para alunos:

- Avise imediatamente um adulto de confiança (pais, responsáveis, professores).
- Mostre a mensagem ou link que causou o problema (não apague nada).
- Não continue conversando com o golpista e não envie mais nada.

Para pais e responsáveis:

- Mantenha a calma e acolha a criança ou adolescente. Culpar só piora a situação.
- Desconecte dispositivos afetados da internet se houver risco de vírus ou acesso remoto.
- Troque senhas das contas envolvidas.
- Avise o banco se dados bancários ou cartões tiverem sido expostos.
- Bloqueie o contato usado para o golpe.
- Denuncie o golpe à Polícia.

Verdade ou Mentira?

Leia as frases abaixo e tente adivinhar: é VERDADE ou MENTIRA?
(Respostas estão na próxima página, mas não vale espiar!)

Frase	Verdade ou Mentira?
É seguro clicar em qualquer link que chega por mensagem de amigos ou familiares.	
Se uma mensagem fala que você ganhou algo, é sempre verdade.	
Colocar fotos com o nome da escola ou uniforme pode ser perigoso.	
Senhas como “123456” e “senha” são fortes e difíceis de descobrir.	
Autenticação em duas etapas ajuda a proteger suas contas.	
Qualquer site na internet é seguro para colocar seus dados.	
É melhor ter uma senha diferente para cada conta.	
Crianças devem pedir ajuda a um adulto quando não souberem se uma mensagem é confiável.	
Compartilhar localização em tempo real nas redes sociais é seguro em qualquer situação.	

Verdade ou Mentira?
RESPOSTAS

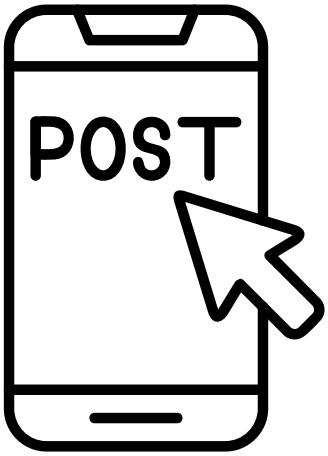
1. ❌ **Mentira – Mesmo mensagens de amigos podem ser resultado de contas invadidas. Sempre desconfie!**
2. ❌ **Mentira – Prêmios falsos são um dos golpes mais comuns!**
3. ✅ **Verdade – Isso pode facilitar a localização da pessoa por estranhos.**
4. ❌ **Mentira – Essas senhas são as primeiras que hackers tentam.**
5. ✅ **Verdade – A autenticação em duas etapas é uma camada extra de segurança.**
6. ❌ **Mentira – Nem todo site é confiável. Verifique sempre se começa com "https" e se é conhecido.**
7. ✅ **Verdade – Usar senhas diferentes evita que uma invasão comprometa tudo.**
8. ✅ **Verdade – Sempre peça ajuda se tiver dúvidas sobre algo que viu online.**
9. ❌ **Mentira – Compartilhar localização pode colocar a sua segurança em risco.**

Lembre-se: o erro não está em cair no golpe,
mas sim em não buscar ajuda
Quanto mais rápido você agir, mais chance
tem de evitar prejuízos!

Uso Consciente das Redes Sociais

As redes sociais fazem parte do nosso dia a dia. Elas conectam, informam, divertem e até ensinam. Mas, para aproveitar tudo isso de forma saudável e segura, é preciso ter consciência e responsabilidade no uso.

- Pense antes de postar
  - Pergunte-se: “eu me sentiria bem se meus pais ou professores vissem isso?”
- Cuidado com o que você vê
  - Nem tudo o que aparece nas redes é real. Filtros, fake news, perfis falsos... Não se compare com o que vê na internet.



- Converse com seus filhos sobre o que eles fazem nas redes. Mostre interesse sem julgar.
- Oriente sobre o que pode ser publicado e incentive o respeito com os outros.
- Verifique a idade mínima dos aplicativos (muitas redes são indicadas apenas para maiores de 13 anos).
- Estabeleça limites de tempo de uso, principalmente antes de dormir e durante as refeições.

Cuidado com o Cyberbullying!

O cyberbullying é quando alguém ofende, humilha ou ameaça outra pessoa pela internet. Pode acontecer por mensagens, comentários, publicações, vídeos ou até memes.

Pode parecer “só uma piada”, mas para quem sofre, dói e machuca muito.

Exemplos de cyberbullying:

- Criar apelidos ofensivos e publicar nas redes
- Compartilhar fotos/vídeos sem autorização
- Mandar mensagens de ódio ou ameaças
- Espalhar fofocas ou mentiras sobre alguém online

Lembre-se: Cyberbullying é crime! Está previsto no Código Penal e na Lei do Bullying Escolar.

Dicas práticas para todos:

Antes de postar, pergunte:

- **Isso é verdadeiro?**
- **Isso é respeitoso?**
- **Isso pode prejudicar alguém?**

Bom uso vs Mau uso das redes sociais

Situação	Bom Uso	Mau Uso
Publicar sobre colegas	Compartilhar conquistas e elogiar com autorização	Zoar, expor fotos sem permissão, fazer piadas maldosas
Criar conteúdo	Postar algo educativo, artístico ou positivo	Criar ou espalhar fake news, vídeos ofensivos ou humilhantes
Participar de grupos	Trocar ideias, estudar junto, combinar atividades	Falar mal dos outros, excluir colegas, enviar mensagens ofensivas
Comentar em posts	Elogiar, apoiar, participar de forma respeitosa	Criticar, debochar ou causar brigas
Compartilhar algo pessoal	Dividir histórias ou conquistas com cuidado e privacidade	Expor momentos íntimos de si ou dos outros

Riscos dos Downloads e Sites de Pirataria

Baixar filmes, jogos, músicas ou programas “de graça” pode parecer vantajoso. Mas quando isso é feito em sites ilegais ou de pirataria, os riscos são grandes — tanto para a segurança do seu dispositivo quanto para a sua privacidade.

- Sites de pirataria podem conter vírus e programas espiões que roubam senhas, fotos e informações.
- Jogos “crackeados” podem deixar seu celular ou computador mais lento ou até inutilizável.

Riscos mais comuns em sites e downloads piratas

Risco	Consequência
Vírus e malware	Invasão do dispositivo, roubo de dados
Phishing (páginas falsas)	Roubo de senhas, golpes financeiros
Programas modificados (cracks)	Espionagem, travamentos, falhas no sistema
Exposição a anúncios indevidos	Conteúdo adulto, jogos de azar, golpes
Riscos legais	Uso e distribuição de conteúdo ilegal é crime

Como identificar um site ou download seguro?

Antes de clicar ou baixar qualquer coisa, vale a pena fazer uma pequena investigação. Aqui vão dicas simples que ajudam a evitar armadilhas:

Faça estas perguntas:

1. O site começa com “https”?
   - O “s” indica que a conexão é segura. Sites sem isso podem ser falsos.
2. O site é conhecido? Já ouvi falar?
   - Desconfie de nomes estranhos, com muitos números, ou com erros de português no endereço.
3. Tem muitos anúncios ou pop-ups pulando na tela?
   - Sites piratas costumam exagerar na quantidade de propagandas.
4. Pede para baixar algo estranho ou instalar complementos?
   - Se não for um site oficial, não instale nada!

Como me manter seguro na internet?

- Antivírus sempre ativo e atualizado
- Extensões de navegador que bloqueiam sites perigosos (como o Web of Trust)
- Controle dos pais em dispositivos usados por crianças
- Atualizações em dia (celular, tablet, computador)

Lembrete importante!

“Navegar com consciência é mais do que evitar vírus — é respeitar a si mesmo e aos outros.”

Uso Responsável da Internet na Escola

A internet pode ser uma grande aliada no aprendizado — quando usada com consciência. Na escola, é fundamental entender quando, como e para que usar a internet, respeitando colegas, professores e o momento de estudo.

✅ **Use a internet como ferramenta de aprendizado**

- Pesquise, tire dúvidas, assista a vídeos educativos e explore conteúdos que complementem o que foi ensinado em sala.

✅ **Siga as orientações dos professores**

- Se a aula for presencial, nem sempre é hora de usar o celular ou o computador. Pergunte antes de acessar qualquer conteúdo.

✅ **Evite distrações**

- Jogos, redes sociais e vídeos aleatórios devem ficar para o horário do recreio ou depois da aula. Durante o estudo, mantenha o foco.

Pode ou não pode?

Situação	Pode	Não Pode
Jogar ou ficar nas redes sociais durante a aula		✕
Fotografar ou filmar colegas sem permissão		✕
Assistir a um vídeo indicado pelo professor	✅	
Pesquisar conteúdo para um trabalho em grupo	✅	

Uso Responsável da Internet na Escola

Cuide dos Equipamentos e Respeite as Configurações

Os computadores, tablets e rede da escola são compartilhados por todos. Por isso:

- Não altere configurações sem autorização (como fundo de tela, programas, senhas, etc.).
- Não instale nem desinstale nada sem permissão.
- Use com cuidado: evite comer ou beber perto dos equipamentos e manuseie com responsabilidade

Respeitar o que é de uso coletivo mostra consciência e colaboração

Fake News e Verificação de Informações

A internet é um mar de informações, mas nem tudo o que circula é verdadeiro. Notícias falsas (fake news) podem confundir, prejudicar pessoas e até causar pânico. Por isso, é importante saber identificar e verificar antes de compartilhar qualquer coisa.

Como identificar uma fake news?

Antes de acreditar ou compartilhar, pergunte-se:

1. A fonte é confiável?
   - Foi publicada por um jornal, site oficial ou especialista no assunto?
   - O site tem muitos anúncios suspeitos ou erros de português?
2. O título parece exagerado ou chocante?
   - Manchetes sensacionalistas tentam chamar atenção, mas podem ser enganosas.
3. A informação aparece em outros sites?
   - Se só um lugar está falando sobre isso, pode ser falso.
4. A notícia tem data e autor?
   - Textos sem data ou sem autor identificado podem ser antigos ou manipulados.
5. Pedem para compartilhar “urgente”?
   - Fake news costumam incentivar o repasse rápido para espalhar desinformação.

Fake News em ação: Bons vs Maus exemplos

Situação	Bom Uso	Mau Uso
Mensagem recebida no WhatsApp	Verificar a fonte e a veracidade antes de compartilhar; duvidar de mensagens alarmistas ou que pedem repasse urgente	Repassar automaticamente sem checar; compartilhar boatos ou informações de fontes não confiáveis
Notícia sobre saúde ou política	Postar algo educativo, artístico ou positivo	Criar ou espalhar fake news, vídeos ofensivos ou humilhantes
Corrente pedindo para divulgar algo urgente	Elogiar, apoiar, participar de forma respeitosa	Criticar ou debochar

O que alunos, pais e professores podem fazer?

👩‍🎓 Alunos: Não compartilhe sem checar. Aprenda a pesquisar e seja um agente da verdade.
👨‍👧 Pais: Conversem com os filhos sobre como identificar notícias falsas e evitem compartilhar conteúdos sem verificar.

Crimes Digitais e Denúncia

A internet não é "terra sem lei". Ações que causam dano, invadem a privacidade ou espalham ódio também são crimes quando acontecem no ambiente digital. É importante saber o que configura crime digital e, principalmente, como se proteger e denunciar.

Exemplos de Crimes Digitais

Situação	É crime?
Invadir redes sociais ou e-mails de outra pessoa	✅ Sim. Invasão de dispositivo
Criar perfis falsos para enganar ou prejudicar alguém	✅ Sim. Falsidade ideológica e difamação
Praticar ou compartilhar bullying virtual (cyberbullying)	✅ Sim. Pode envolver várias infrações
Espionar a câmera ou microfone de outra pessoa com programas ocultos	✅ Sim. Violação de privacidade e espionagem
Criar ou compartilhar boatos falsos sobre alguém (fake news pessoais)	✅ Sim. Calúnia e difamação
Baixar e distribuir conteúdo pirata (filmes, jogos, músicas)	✅ Sim. Violação de direitos autorais

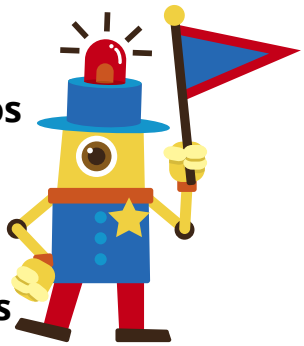
O que fazer em caso de crime digital?

Se você, um amigo, colega ou familiar for vítima de algo assim:

- **Salve as provas: prints, links, datas e mensagens.**
- **Não responda à provocação: isso pode piorar ou ser usado contra você.**
- **Converse com um adulto de confiança: pais, professores ou responsáveis.**
- **Faça uma denúncia:**

Onde denunciar?

- **Polícia Civil – Delegacia de Crimes Cibernéticos**
- **Plataformas e redes sociais – Todas têm mecanismos de denúncia interna**
- **SaferNet Brasil – www.safernet.org.br (anônima e especializada em crimes virtuais)**
- **Disque 100 – Para denúncias de violações de direitos humanos, inclusive digitais**



Lembre-se!

- **Nem tudo que "parece brincadeira" é inofensivo.**
- **A liberdade de expressão não é desculpa para ofender ou causar mal.**
- **A internet deve ser usada com respeito, ética e responsabilidade.**

Quem comete crimes digitais também pode responder legalmente, mesmo sendo menor de idade.

Vamos praticar a Cidadania Digital?

Seguir boas práticas de segurança digital é essencial para garantir um ambiente online mais seguro e respeitoso para todos. A internet pode ser um lugar incrível para aprender, se expressar e se conectar, desde que usada com consciência!

Lembre-se!

🔐 Proteja suas informações pessoais
💬 Seja respeitoso em todas as interações online
📚 Verifique as informações antes de compartilhar
🚫 Denuncie conteúdos perigosos, ofensivos ou ilegais
🤝 Ajude os outros a usarem a internet com responsabilidade

Compartilhe!

🔄 Quanto mais pessoas souberem, mais segura será a internet para todos.
🌍 Você também é responsável por um ambiente digital saudável!


25 DE MARÇO
CAÇADOR
DE 1934