



Cyber Day 2026

Preparado pela área de L&D da KPMG

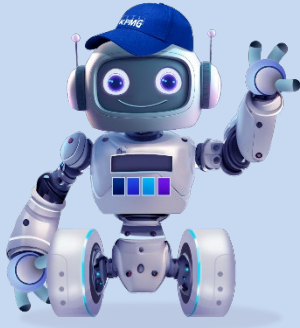
Apostila do Aluno – Princípios Básicos



Este documento é uma apostila elaborada para os participantes do treinamento presencial. Ela inclui um detalhamento de cada tópico com os principais conceitos abordados no treinamento, juntamente com detalhes sobre a atividade e perguntas de reflexão, além de dicas e orientações para garantir a retenção do aprendizado.

Este documento está formatado para ser impresso em papel A4.

Como usar esta apostila



Olá!

Eu sou o **Cyber Buddy**, seu amigo e guia para ajudá-lo a entender como estar seguro on-line, e como proteger a si mesmo e suas informações pessoais ao usar a internet.

Tudo o que você aprendeu na sessão do **Cyber Day** foi reunido nesta apostila. Isso inclui algumas ótimas dicas sobre como você pode usar a tecnologia com segurança, como estar seguro nas mídias sociais, como proteger seus dispositivos eletrônicos e como usar seu tempo de tela de maneira consciente.

Ele também inclui algumas atividades que você pode completar em sala de aula durante a sessão e, se não der tempo, em casa durante seu tempo livre.

Esperamos que a sessão do Cyber Day conosco tenha sido divertida e informativa.

Use esta apostila para lembrar todas as diretrizes de segurança que discutimos em aula hoje.

Seja inteligente. Seja social. Esteja seguro.

Bem-vindo ao Cyber Day!

O que são riscos cibernéticos?

- Conteúdo impróprio
- Contato com pessoas desconhecidas
- Perda do acesso a imagens e músicas
- Postagem de informações privadas
- Golpes
- Dados corrompidos
- Cyberbullying
- Download accidental de malware
- Sistemas danificados
- Vício em jogos
- Vício em mídias sociais
- Dados pessoais roubados

Conheça a sua atuação digital

Sua **pegada digital** é tudo o que você faz online!



Toda vez que você fica online, você deixa um registro digital permanente que pode ser visível para outras pessoas.

Quais informações você nunca deve compartilhar on-line?

Quais são alguns exemplos de "informações pessoais"?

Escreva sua resposta aqui.

Quais informações você nunca deve compartilhar on-line?	Escreva sua resposta aqui.
Você pode compartilhar as informações pessoais da sua família ou dos seus amigos online?	Escreva sua resposta aqui.
Você acha que tudo o que você posta online permanece privado?	Escreva sua resposta aqui.

Quais informações você pode compartilhar on-line?

Escreva sua resposta aqui.



O que você compartilha online, fica online! Portanto, tenha cuidado com a sua pegada digital.

Certifique-se de que o que você compartilha é seguro, responsável e respeitoso. Se você não tiver certeza do que fazer, peça orientações a um adulto de confiança.

Uso de mídias sociais, mas de forma segura

As mídias sociais são uma maneira rápida e conveniente de permanecer em contato com a família e com os amigos, compartilhar notícias e postar fotos. Se você não tiver cuidado com a forma como utiliza as mídias sociais, elas também são um meio fácil para os cibercriminosos aprenderem mais sobre você.



Muitos governos em todo o mundo estão aumentando a idade a partir da qual as crianças podem ter acesso às mídias sociais. Isso é para garantir que você esteja seguro online.

Atividade: Uso de mídias sociais, mas de forma segura

Cenário Um

Emily está fazendo uma pequena pausa em um jogo online. De repente, ela recebe um pedido de amizade de uma pessoa que ela não conhece. **Emily deve aceitar o pedido de amizade?**

☐

Sim

☐

Não

Justifique sua resposta.

Cenário Dois

Alex tira uma foto divertida com os seus amigos em uma festa de aniversário e depois posta a foto nas redes sociais. **O que Alex esqueceu de fazer e por que isso é importante?**

Escreva sua resposta aqui.

Cenário Três

Anya está pensando em criar um perfil nas redes sociais. Ela não tem certeza se deve deixar seu perfil visível para todos. **O que você vai sugerir a Anya? Justifique sua resposta.**

Escreva sua resposta aqui.

Saber como usar as redes sociais com segurança é um elemento importante para se proteger online.

Siga estas dicas de segurança nas redes sociais.



Um passo à frente dos hackers

O que fazer e o que não fazer em relação a senhas



O que fazer

- Crie uma senha forte. Uma senha forte deve conter frases, números, símbolos, uma combinação de letras maiúsculas e minúsculas, por exemplo: 'Eu comi 22 fatias de pizza na minha festa de aniversário! — **Ec22fdpnmfda!**
- Crie uma senha que seja exclusiva para você – torne-a fácil de lembrar, mas mais difícil de hackear!
- Use uma frase secreta que tenha pelo menos 4 palavras e 12 caracteres.
- Crie senhas diferentes para cada conta.
- Use a autenticação multifator para aumentar a segurança.



O que não fazer

- Não inclua informações pessoais, como nomes de membros da família ou de animais de estimação, endereços, números de telefone ou datas de aniversário em sua senha.
- Não use senhas simples e fáceis de adivinhar como "senha" ou "1234". Torne-as únicas.
- Não anote senhas ou compartilhe-as com seus amigos.
- Não ignore os prompts que pedem que você altere senhas.

Qual das senhas a seguir é a mais segura? Assinale a resposta correta.

- ☐ l822sop@mbp!
- ☐ Theskyisblue
- ☐ B@tm@n1&Rob!n
- ☐ 0123%456

Há algum problema em compartilhar senhas com seu melhor amigo? Justifique sua resposta.

Bem-estar digital: O cuidado consigo mesmo



Aqui está um fato interessante, depois de frequentar a escola, fazer a lição de casa, dormir e fazer as refeições, em média as crianças têm apenas 4 horas de tempo livre por dia. São 62 dias por ano!

Se você estiver movendo a barra de rolagem por mais de três horas por dia, isso significa que está usando a maior parte do seu tempo livre em dispositivos eletrônicos.

Quais outras atividades você poderia realizar em vez disso?

Escreva suas ideias aqui.

O que me faz ficar direto no celular ou em outros dispositivos eletrônicos?

Escreva exemplos de alguns fatores de distração que fazem você voltar a olhar seus dispositivos eletrônicos.

Como você pode quebrar o ciclo vicioso e reduzir o tempo gasto em dispositivos eletrônicos?

Escreva suas ideias aqui.

--

Bem-estar digital: O cuidado com a sociedade

Quando você passa muito tempo nas telas, isso significa que você está perdendo outras atividades, como se divertir ou passar tempo com os amigos e familiares.

Como você gostaria de passar o tempo com sua família e amigos?

Quais atividades vocês podem realizar juntos?

Escreva suas ideias aqui.

How is communicating online different than talking in-person?



In-person

- **Non-verbal cues:** Body language and facial expressions convey meaning.
- **Tone of voice:** Show warmth, anger, excitement.
- **In-person:** Enhances connection and engagement.
- **More effort:** Takes more time and planning to meet with someone.



Online

- **No verbal cues:** Barrier to connection and misunderstandings.
- **No audible cues:** Barrier to clarity of message.
- **Inability to give feedback:** Misunderstandings can escalate.
- **Online is easier:** There's less effort to engage meaningfully. You can multi-task at the same time.

Vs

Cyberbullying

Os seus colegas de classe estão enviando mensagens de texto em um grupo com comentários ofensivos sobre outra pessoa. Você está nesse grupo e está recebendo essas mensagens. O que você faz. **O que você faz? Selecione todas as opções aplicáveis.**

- | | |
|--------------------------|--|
| ☐ | Participe da conversa |
| ☐ | Ignore e apague as mensagens |
| ☐ | Não responda às mensagens, mas salve-as para mostrá-las a um adulto de confiança |

Justifique sua resposta.

Aqui estão algumas dicas a seguir se você estiver sofrendo cyberbullying.

	Não responda nem reaja		Mantenha sua privacidade
	Bloqueie o agressor		Relate o ocorrido a um adulto de confiança

Como você pode mostrar seu apoio a alguém que está sofrendo cyberbullying? Siga essas dicas!

	Dê apoio à pessoa que é alvo do cyberbullying		Tenha uma postura firme em relação ao cyberbullying
	Denuncie o cyberbullying		Não participe do cyberbullying



Oi!

Aprendemos muitas coisas hoje, algumas das quais você já sabia e outras que eram novas. Espero que você tenha achado a sessão útil e interessante!

Aqui vão algumas dicas rápidas que você pode aplicar quando utilizar os seus dispositivos eletrônicos.

Lembre-se: seja inteligente, seja social e seguro!

Felicitações!

Lembre-se destas dicas:

Use a tecnologia com segurança • Crie senhas fortes • Mantenha os dispositivos atualizados • Tenha cuidado ao clicar em algum conteúdo	Seja o verdadeiro VOCÊ online • Não pratique bullying • Cuide dos outros online • Seja genuíno e autêntico
Refleta sobre a privacidade • Contate apenas seus amigos • Verifique as configurações de privacidade • Respeite a privacidade dos outros • Evite compartilhar informações pessoais • Parta do pressuposto de que todas as mensagens e postagens nas mídias sociais podem ser vistas por qualquer pessoa	Cuide-se • Evite visualizar telas antes de dormir • Reduza o som de notificações • Faça pausas para estar online • Pare com os maus hábitos



Obtenha ajuda: Na dúvida, peça sempre ajuda a um adulto de confiança!

© 2026 Os direitos autorais são de propriedade de uma ou mais entidades da KPMG International. As entidades da KPMG International não prestam serviços a clientes. Todos os direitos reservados.

O nome KPMG e o seu logotipo são marcas utilizadas sob licença pelas firmas-membro independentes da organização global KPMG.

KPMG refere-se à organização global ou a uma ou mais firmas-membro da KPMG International Limited (“KPMG International”), cada uma das quais é uma entidade legal separada. KPMG International Limited é uma empresa inglesa privada de responsabilidade limitada e não presta serviços a clientes. Para mais detalhes sobre a nossa estrutura, acesse <https://kpmg.com/xx/en/misc/governance.html>.

Todas as informações apresentadas neste documento são de natureza genérica e não têm por finalidade abordar as circunstâncias de um indivíduo ou entidade específicos. Embora tenhamos nos empenhado em prestar informações precisas e atualizadas, não há nenhuma garantia sobre a exatidão das informações na data em que forem recebidas ou em tempo futuro. Essas informações não devem servir de base para se empreender ação alguma sem orientação profissional qualificada e adequada, precedida de um exame minucioso da situação concreta.