



Cyber Day 2026

Preparado pela área de L&D da KPMG

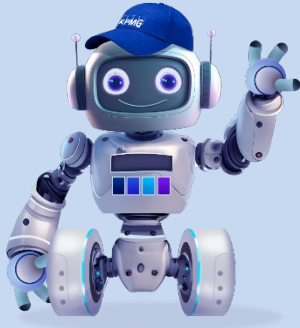
Apostila do Aluno - Avançado



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 de ataques cibernéticos e os prós e contras da Inteligência Artificial. Há dicas sobre como usar os dispositivos de forma consciente e equilibrar o tempo gasto nas telas para que você cultive outros hobbies e tenha tempo de qualidade com amigos e familiares.

Ele também inclui algumas das atividades e cenários 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

Recapitulação dos fundamentos de segurança!

Como proteger seu dispositivo eletrônico

Cenário 1:

Andy está trabalhando com quatro de seus colegas de classe em uma breve apresentação em vídeo que está prevista para acontecer no dia seguinte. Um colega da equipe compartilha um link para um pacote premium de modelos de edição de vídeo que ele encontrou em um post de um criador de conteúdo. O post tem muitas curtidas, comentários como “deu certo para mim” e uma contagem regressiva dizendo que o download gratuito termina em 20 minutos.

Andy abre o link em seu notebook. O site parece bem elaborado, mas o endereço eletrônico é um pouco diferente do endereço eletrônico da página oficial do criador. O site pede a Andy para criar uma conta gratuita antes de baixar os modelos. Um banner também pede que Andy instale uma extensão do navegador para “desbloquear downloads mais rápidos”.

Quando Andy clica em fazer download, uma janela pop-up diz que o navegador bloqueou um arquivo porque ele “pode não ser seguro”.

Ao mesmo tempo, o notebook de Andy mostra um lembrete de atualização do sistema, a qual ele postergou várias vezes, pois o aviso sempre aparecia quando Andy estava ocupado. O aplicativo antivírus de Andy também mostra que a última verificação completa foi há mais de um mês.

A configuração de segurança do navegador está atualmente definida como básica, de modo que cookies e pop-ups de terceiros são permitidos.

Os companheiros de equipe de Andy estão ficando impacientes. Andy não tem certeza se deve continuar, alterar as configurações, usar uma senha rápida ou procurar outra opção.

O prazo está próximo, o grupo está dependendo dele, e a escolha mais segura pode atrasar todo mundo.

Perguntas:

1. Quais pistas sugerem que esse site pode não ser seguro, mesmo que pareça profissional?
2. Andy deve parar por um momento e instalar a atualização do sistema ou continuar trabalhando porque o prazo está próximo? Explique o risco de atrasar as atualizações de segurança.
3. Andy deve diminuir o nível das configurações de segurança do navegador, permitir pop-ups, ou instalar a extensão para concluir o download? Quais configurações mais seguras ele deve usar em vez disso?
4. Se Andy criar uma conta, o que ele deve evitar fazer com a senha que ele deve criar? Qual seria uma opção de senha mais forte?
5. O que Andy pode sugerir ao grupo para que eles terminem o projeto sem baixar recursos de uma fonte arriscada?
6. O que você faria se estivesse no lugar de Andy?

Discuta as perguntas atribuídas ao seu grupo. Registre suas respostas ou observações no espaço abaixo.

Cenário 2:

Mia recebe uma solicitação de “follow” de uma pessoa que parece ter mais ou menos sua idade. O perfil dessa pessoa parece normal. Elas seguem páginas semelhantes, compartilham posts sobre os mesmos hobbies e têm alguns seguidores em comum.

Elas começam a conversar casualmente sobre filmes, músicas e um hobby de que ambas gostam. A pessoa então pergunta a Mia sobre os lugares perto da casa de Mia aos quais ela mais gosta de ir. Ao longo da semana seguinte, as conversas parecem acontecer de forma natural e divertida. A pessoa diz a Mia que é muito bom conversar com ela, pois a conversa flui de forma leve e descomplicada, e menciona coisas que Mia disse. Mia se sente bem com a interação. É bom ter alguém que parece ouvir de verdade o que você fala.

Depois de alguns dias, a pessoa diz: “Este aplicativo é irritante porque as mensagens acabam se perdendo. Eu costumo usar este outro aplicativo privado de mensagens; nossos pais não podem nos espionar por lá!”

Com o passar do tempo, a pessoa começa a insistir para que Mia use o aplicativo privado de mensagens. Se Mia responde às mensagens bem depois de elas serem enviadas, a pessoa diz coisas como: “Nossa, onde você estava? Senti muito a sua falta”. E isso faz com que Mia se sinta um pouco pressionada a responder rapidamente às mensagens dessa pessoa.

Quando Mia sugere adicionar alguns de seus amigos ao aplicativo, a pessoa responde: “Ah, não vamos fazer isso. Prefiro manter a conversa somente entre nós, gosto que a nossa amizade seja exclusiva!”

A pessoa manda sua foto para Mia e quer que Mia envie sua foto também. Quando Mia hesita, a pessoa parece ficar irritada e diz que Mia não confia nela, caso contrário, por que ela hesitaria?

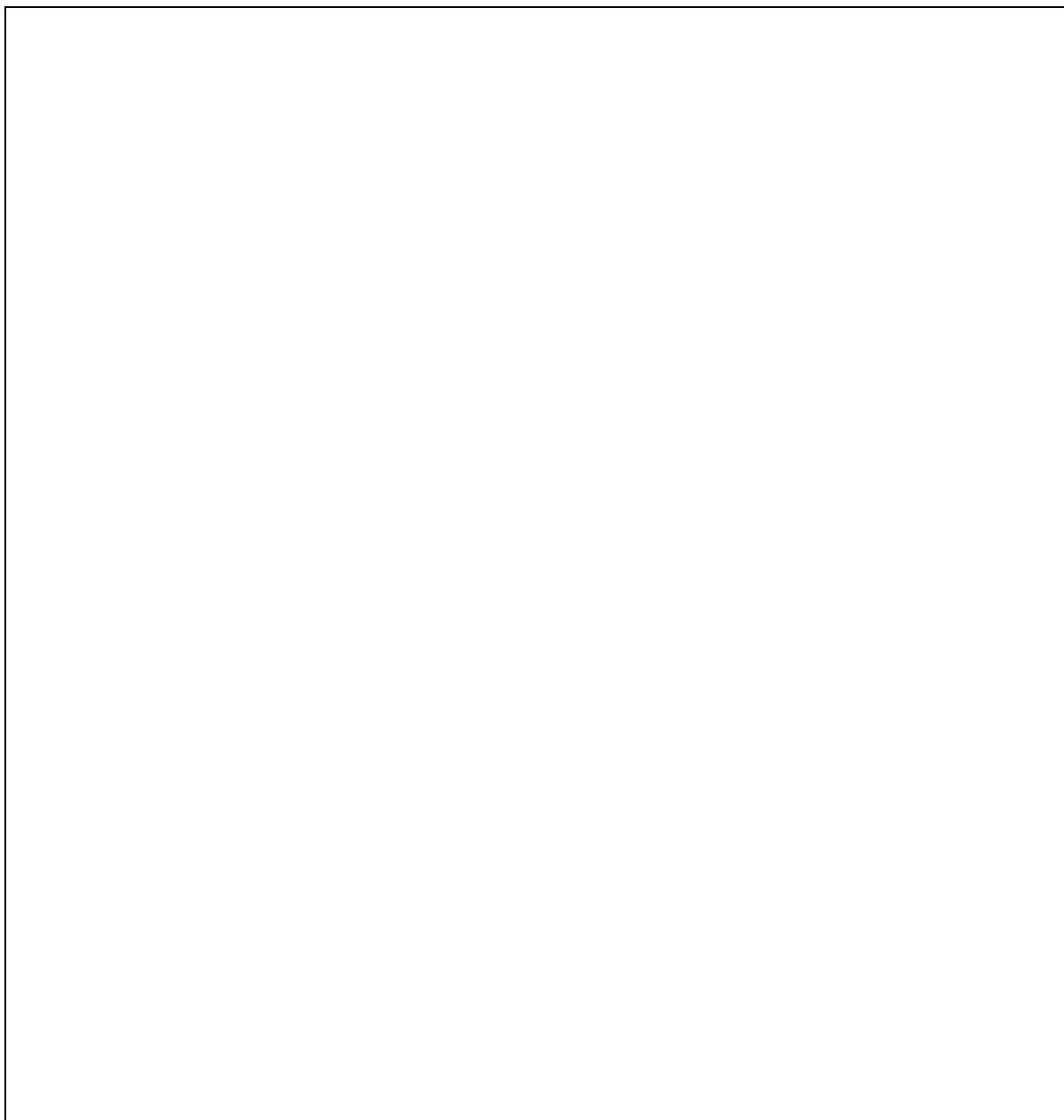
Mia não sabe como se sente a respeito disso. A foto que a pessoa compartilhou não é inapropriada e é justo que Mia envie uma foto sua a essa pessoa também. Mia está começando a se sentir um pouco acuada e um pouco menos entusiasmada com as interações nos últimos dias.

Mas ela se pergunta se está “encanando demais com isso”.

Perguntas:

1. O que você acha de Mia responder ao pedido de amizade recebido – isso parece seguro e normal para você? Justifique sua resposta.
2. A pessoa diz a Mia que é muito bom conversar com ela, pois a conversa flui de forma leve e descomplicada, e se abre emocionalmente. Isso é um sinal de que a pessoa quer apenas ser amigável ou pode ser um sinal de alerta? O que Mia deve observar?
3. A pessoa também sugere mudar para um aplicativo privado de mensagens. O que Mia deve fazer? O que há de arriscado nesse pedido?
4. O que você acha sobre a pessoa pedir para manter as conversas apenas entre Mia e ela e evitar conversas em grupo?
5. Por que pode ser um sinal de alerta se alguém quiser manter Mia longe de seus amigos?
6. O que você faria se estivesse no lugar de Mia?

Discuta as perguntas atribuídas ao seu grupo. Registre suas respostas ou observações no espaço abaixo.





Inteligência Artificial (IA):

A IA tornou-se parte do nosso dia-a-dia – desde as recomendações das redes sociais que recebe no celular, passando por assistentes virtuais como a Siri, Alexa ou Google Assistente, até o Chat GPT com os quais todos estão familiarizados e até os robôs de última geração. A IA causou um enorme impacto em nossas vidas!

A IA funciona com base em redes neurais, reconhecendo padrões em grandes quantidades de dados, como nossos posts nas mídias sociais, o histórico de compras online, as músicas mais tocadas e quase tudo o que inserimos como dados em nossos dispositivos eletrônicos.



Como usar a IA de forma segura?

Aqui estão algumas dicas para ajudar a mantê-lo seguro on-line.

	✓ Esteja atento às informações pessoais
	✓ Entenda as configurações de privacidade
	✓ Não compartilhe informações em excesso

	✓ Pense de maneira crítica
	✓ Seja cauteloso em relação às mensagens geradas por IA
	✓ Mantenha-se informado

Refleta!

Mary precisa terminar um resumo de livro para o projeto de clube do livro. O vencimento do prazo está próximo, então ela usa o ChatGPT para criar um resumo rápido. Ela adiciona o resumo gerado por IA à sua apresentação sem conferi-lo com o livro. Durante o encontro com o grupo, os demais membros apontam que alguns dos personagens e eventos descritos na apresentação de Mary não estão presentes no livro.

Qual é o termo para quando a IA inventa informações ou descreve coisas que não são verdadeiras?

Assinale a resposta correta.

- ☐ Delírio
 ☐ Imaginação
 ☐ Alucinação
 ☐ Inspiração

Os ataques cibernéticos — Tenha cuidado!

Diferentes tipos de ataques cibernéticos

Vírus e worms	Ataque a dicionário	Spyware e adware	Ransomware e DDoS
Um vírus de computador se espalha de um hospedeiro a outro e tem a perigosa capacidade de se replicar.	Um ataque de dicionário é usado para decifrar senhas.	Spywares são aplicativos que obtêm informações confidenciais sobre as atividades de outra pessoa no computador por meio da transferência secreta de dados do disco rígido.	Ransomware é um tipo de malware que ameaça publicar os dados da vítima, ou bloqueia o acesso a tais dados, a menos que a vítima pague um resgate.
Um worm funciona da mesma forma que um vírus. Ele pode se espalhar para outros computadores automaticamente.	A decifração da senha é o processo de tentar obter acesso não autorizado a sistemas restritos usando senhas comuns ou algoritmos que adivinham senhas.	Adwares são aplicativos que exibem ou baixam automaticamente material publicitário indesejado quando um usuário está online.	O Ataque Distribuído de Negação de Serviço (DDoS) é um ataque cibernético que torna uma máquina ou rede indisponível para seus usuários, interrompendo os serviços.

Como reconhecer sinais de um ataque cibernético

Analise os exemplos a seguir e identifique se eles podem ser sinais de um ataque cibernético ou problemas técnicos comuns. Escreva suas respostas na tabela.

Evidência	Possível sinal de ataque cibernético ou problema técnico comum?	Por que você acha isso?
Um e-mail de um remetente desconhecido diz: "Clique aqui agora para manter sua conta ativa".		
A bateria do seu notebook está quase acabando.		
Uma mensagem informa que sua senha foi alterada, mas você não a alterou.		
Você não está conseguindo acessar a sua conta, mesmo que você tenha conseguido acessá-la utilizando a mesma senha ontem.		
Continuam aparecendo pop-ups que dizem: "Seu dispositivo está infectado!"		
Sua internet está lenta, enquanto várias pessoas na sua casa estão transmitindo vídeos.		
Sua internet fica excepcionalmente lenta depois que a transmissão para.		

Evidência	Possível sinal de ataque cibernético ou problema técnico comum?	Por que você acha isso?
Uma atualização de jogo leva mais tempo do que o esperado para ser instalada.		

Ataques cibernéticos: Principais conclusões

Sinais de um ataque cibernético	Como se recuperar de um ataque	Como evitar ataques cibernéticos
- E-mails estranhos ou misteriosos - Mensagens sobre a alteração da sua senha - Bloqueio de uma conta ou um dispositivo - Pop-ups suspeitos ou estranhos - Conexões mais lentas do que o normal - Sempre verifique com um adulto de confiança se você suspeitar de problemas!	- Altere suas senhas - Determine o que foi perdido ou comprometido - Notifique seus contatos - Siga as etapas de recuperação do antivírus - Faça o backup de arquivos - Verifique com um adulto de confiança a respeito do problema	- Certifique-se sempre de que suas senhas sejam fortes. - Fique atento a aplicativos desconhecidos, mensagens ou pop-ups estranhos. - Use uma rede segura de Wi-Fi e evite Wi-Fi gratuito em locais públicos. - Certifique-se de que o software esteja atualizado e habilite os recursos de segurança e os programas antivírus corretos.

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?

Se eu tivesse mais tempo livre, eu gostaria de...

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?

O que posso mudar para me ajudar a alcançar meus objetivos?

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.

Cyberbullying

Cenário 1:

Em um chat do grupo da escola, alguém compartilha um print de tela constrangedor de uma chamada de vídeo em que a câmera de um aluno congela no momento errado. No início, as pessoas reagem com emojis de riso e fazem piadas internas. Em seguida, alguns alunos começam a adicionar legendas, repostar o print de tela em um chat com um número menor de membros e marcar outras pessoas para que elas “avaliem” esse print de tela. O aluno que aparece nesse print de tela envia uma mensagem dizendo: “Vocês podem, por favor, apagar isso?”, mas as piadas continuam. Um colega quer defendê-lo chamando todos no grupo, enquanto outro acha que seria melhor salvar as mensagens, checar em particular com o aluno e pedir ajuda a um adulto ou professor de confiança.

Perguntas:

1. Onde o comportamento da pessoa cruza os limites do razoável? Quando isso deixa de ser uma piada e se torna cyberbullying?
2. Por que os alunos podem continuar rindo ou compartilhando mesmo que saibam que isso parece ser errado?
3. Na qualidade de alguém que participa do chat em grupo, qual é a primeira coisa que você fará? Explique o motivo.
4. O que você faria se sofresse cyberbullying?

Discuta as perguntas atribuídas ao seu grupo. Registre suas respostas ou observações no espaço abaixo.



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

Cenário 2:

Mais tarde naquela noite, o print de tela compartilhado no chat do grupo da escola aparece novamente - desta vez em um chat menor de um jogo do qual alguns colegas desse grupo estão participando juntos. Algumas pessoas fazem piadas sobre o aluno que aparece no print de tela. Um jogador muda seu nome de usuário para copiar o nome do aluno como uma piada e outro sugere usar o print de tela como um meme no chat da aula de amanhã. Outro aluno que também está participando do jogo se sente desconfortável com a situação porque o aluno que aparece no print de tela já havia pedido a todos que apagassem o print. O aluno que está se sentindo desconfortável quer demonstrar seu apoio ao aluno que está sofrendo cyberbullying, mas também se preocupa, pois, se falar alguma coisa para defendê-lo, o grupo dirá que ele está exagerando ou tentando acabar com a diversão.

Perguntas:

1. Se você fosse o aluno vendo isso acontecer, o que você faria primeiro? Explique o motivo.
2. Quem você escolheria ser? Uma pessoa que só observa a situação (assistindo em silêncio) ou uma pessoa que adota uma postura firme em relação ao cyberbullying (coletando evidências para depois relatar o ocorrido a um adulto)? Por quê?
3. Crie uma breve mensagem de apoio ao aluno sem intensificar a discussão.
4. Crie um breve relatório sobre esse incidente que você pode compartilhar com um adulto de confiança. Quais detalhes você incluirá no relatório / excluirá do relatório?

Discuta as perguntas atribuídas ao seu grupo. Registre suas respostas ou observações no espaço abaixo.

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.