

CENTRO EDUCACIONAL ALAMEDA ARGENTINA
REVISÃO 7º ANO - 3º BIMESTRE
ATIVIDADE RESPONDIDA / GABARITO

1. O que é cyberbullying?

- A) Uma agressão psicológica praticada por meios digitais
- B) Uma brincadeira realizada apenas na escola
- C) Um problema exclusivamente físico
- D) Uma forma de proteger contas online

Resposta: A) Uma agressão psicológica praticada por meios digitais

2. Cite duas formas comuns de cyberbullying.

Resposta: Mensagens ofensivas, compartilhamento de fotos ou vídeos constrangedores sem autorização, perfis falsos, boatos ou exclusão social digital.

3. Uma diferença entre bullying e cyberbullying é que o cyberbullying:

- A) Só ocorre dentro da escola
- B) Pode ocorrer no ambiente virtual e a qualquer hora
- C) Nunca pode ser anônimo
- D) Atinge apenas uma pessoa

Resposta: B) Pode ocorrer no ambiente virtual e a qualquer hora

4. Cite duas atitudes que ajudam a combater o cyberbullying.

Resposta: Denunciar, bloquear o agressor, guardar provas, procurar um adulto de confiança e praticar educação digital.

5. Qual situação representa cyberbullying?

- A) Estudar em grupo pela internet
- B) Criar um perfil falso para humilhar alguém
- C) Assistir a uma aula online
- D) Jogar com amigos

Resposta: B) Criar um perfil falso para humilhar alguém

6. Qual alternativa apresenta um exemplo de dado pessoal?

- A) CPF
- B) Nome de um planeta
- C) Modelo de um jogo
- D) Nome de uma disciplina

Resposta: A) CPF

7. O que é um vazamento de dados?

Resposta: É a exposição de informações pessoais sem autorização, por falha de segurança, ataque ou negligência.

8. Segundo o conteúdo, qual é um exemplo de dado sensível?

- A) Número de matrícula
- B) Religião
- C) Nome completo
- D) Telefone

Resposta: B) Religião

9. Cite duas consequências possíveis de um vazamento de dados.

Resposta: Roubo de identidade, fraudes financeiras, exposição da privacidade, phishing, engenharia social ou sequestro de contas.

10. Qual prática ajuda a proteger dados pessoais?

- A) Usar a mesma senha em todos os sites
- B) Clicar em qualquer link recebido
- C) Ativar a verificação em duas etapas
- D) Compartilhar dados em redes públicas

Resposta: C) Ativar a verificação em duas etapas

11. A sigla LGPD significa:

- A) Lei Geral de Proteção de Dados
- B) Lei Global de Programas Digitais
- C) Lista Geral de Proteção Digital
- D) Lei Geral de Programação de Dados

Resposta: A) Lei Geral de Proteção de Dados

12. Cite dois cuidados para proteger seus dados na internet.

Resposta: Usar senhas fortes e diferentes, ativar verificação em duas etapas, evitar links desconhecidos, não compartilhar dados em redes públicas e manter sistemas atualizados.

13. Golpes e fraudes online procuram principalmente:

- A) Melhorar a velocidade da internet
- B) Obter dinheiro, dados pessoais ou acesso a contas
- C) Ensinar segurança digital
- D) Atualizar programas automaticamente

Resposta: B) Obter dinheiro, dados pessoais ou acesso a contas

14. O que é phishing?

Resposta: É um golpe que usa e-mails, sites ou mensagens falsas que imitam fontes confiáveis para roubar dados.

15. Qual é um sinal comum de tentativa de fraude?

- A) Mensagem sem urgência e de fonte confirmada
- B) Link verificado e conhecido
- C) Pressão para agir rapidamente
- D) Uso de autenticação em duas etapas

Resposta: C) Pressão para agir rapidamente

16. No golpe do WhatsApp clonado, criminosos podem:

- A) Pedir dinheiro aos contatos da vítima
- B) Atualizar o celular da vítima
- C) Instalar antivírus gratuitamente
- D) Criar cópias de segurança

Resposta: A) Pedir dinheiro aos contatos da vítima

17. O que você deve fazer ao receber uma mensagem suspeita pedindo dinheiro com urgência?

Resposta: Não clicar em links nem enviar dinheiro imediatamente; confirmar a identidade do remetente por outro meio, bloquear e denunciar se for golpe.

18. Antes de pagar um boleto recebido pela internet, é importante:

- A) Pagar rapidamente sem conferir
- B) Conferir os dados do boleto e do beneficiário
- C) Enviar o boleto para desconhecidos
- D) Desativar a segurança do navegador

Resposta: B) Conferir os dados do boleto e do beneficiário

19. Cite dois cuidados ao fazer compras pela internet.

Resposta: Verificar a reputação da loja, conferir o endereço do site, preferir sites conhecidos e não comprar por links desconhecidos.

20. Fake news são:

- A) Notícias falsas criadas para enganar, manipular ou gerar cliques
- B) Todas as notícias publicadas na internet
- C) Somente erros de digitação
- D) Mensagens particulares entre amigos

Resposta: A) Notícias falsas criadas para enganar, manipular ou gerar cliques

21. Cite dois fatores que ajudam as fake news a se espalhar.

Resposta: Compartilhamento sem checagem, títulos sensacionalistas, conteúdo manipulador ou apelativo e perfis falsos ou robôs.

22. Qual pode ser uma consequência da desinformação?

- A) Aumento automático da segurança digital
- B) Confusão e medo na população
- C) Fim dos golpes virtuais
- D) Proteção automática da privacidade

Resposta: B) Confusão e medo na população

23. Ao receber uma notícia duvidosa, a atitude mais adequada é:

- A) Compartilhar imediatamente
- B) Ler apenas o título
- C) Verificar a fonte e pesquisar antes de compartilhar
- D) Enviar para todos os grupos

Resposta: C) Verificar a fonte e pesquisar antes de compartilhar

24. O que devemos verificar antes de compartilhar uma notícia?

Resposta: A fonte, o conteúdo além do título e a confirmação da informação em fontes confiáveis ou de checagem.

25. Títulos sensacionalistas podem ser um sinal de:

- A) Fake news ou conteúdo manipulador
- B) Senha forte
- C) Autenticação em duas etapas
- D) Atualização de sistema

Resposta: A) Fake news ou conteúdo manipulador

26. Cite dois efeitos negativos das fake news na sociedade.

Resposta: Confusão, medo, desinformação, conflitos sociais, desconfiança na ciência e instituições ou problemas de saúde pública.

27. O que é exposição excessiva na internet?

- A) Compartilhar informações demais sobre a vida pessoal
- B) Usar uma senha forte
- C) Atualizar aplicativos
- D) Bloquear um perfil falso

Resposta: A) Compartilhar informações demais sobre a vida pessoal

28. Cite dois riscos da exposição excessiva nas redes sociais.

Resposta: Furto ou roubo, clonagem de identidade, assédio, perseguição online e perda de privacidade.

29. Qual comportamento é mais seguro nas redes sociais?

- A) Publicar o endereço residencial

- B) Mostrar documentos em vídeos
- C) Limitar quem pode visualizar suas postagens
- D) Compartilhar localização em tempo real com todos

Resposta: C) Limitar quem pode visualizar suas postagens

30. Cite duas maneiras de proteger sua privacidade digital.

Resposta: Configurar a privacidade das redes, evitar divulgar rotina e localização, não aceitar estranhos, revisar quem vê as publicações e não postar documentos.

31. Postar a localização em tempo real pode:

- A) Aumentar a segurança automaticamente
- B) Expor a rotina e criar riscos à segurança
- C) Impedir golpes
- D) Proteger documentos pessoais

Resposta: B) Expor a rotina e criar riscos à segurança

32. Por que é importante pensar antes de publicar algo na internet?

Resposta: Porque o conteúdo pode ser salvo, copiado, compartilhado e até usado de forma mal-intencionada.

33. Qual alternativa reúne duas boas práticas de segurança digital?

- A) Senha forte e autenticação em duas etapas
- B) Senha repetida e localização pública
- C) Links desconhecidos e perfil aberto
- D) Documentos publicados e senha curta

Resposta: A) Senha forte e autenticação em duas etapas

34. Explique por que não devemos clicar em links desconhecidos.

Resposta: Porque podem levar a páginas falsas, instalar conteúdo malicioso ou ser usados em golpes para roubar dados e contas.

35. Qual atitude resume melhor um uso responsável da internet?

- A) Compartilhar tudo rapidamente
- B) Verificar informações, proteger dados e respeitar outras pessoas
- C) Aceitar qualquer pessoa nas redes
- D) Usar a mesma senha em todos os serviços

Resposta: B) Verificar informações, proteger dados e respeitar outras pessoas