

Privacidade e Dados Pessoais

7.º Ano

TIC

3 páginas

Competências que desenvolve: Conhecer comportamentos que visam a proteção da privacidade; adotar comportamentos seguros na utilização de ferramentas digitais.

1. Dados pessoais — conceitos

- 1.1. O que são dados pessoais? Apresenta 3 exemplos.
- 1.2. Por que é importante proteger os dados pessoais online?
- 1.3. Apresenta 2 riscos de partilhar dados pessoais na internet.
- 1.4. O que é a RGPD? Qual é o seu objetivo?

2. Privacidade digital

- 2.1. Apresenta 3 estratégias para proteger a privacidade online.
- 2.2. O que são as definições de privacidade nas redes sociais?
- 2.3. Por que é importante rever as definições de privacidade regularmente?
- 2.4. Apresenta 2 exemplos de informação que NÃO se deve partilhar publicamente.

3. Segurança de contas

- 3.1. O que é a autenticação de dois fatores? Por que é importante?
- 3.2. Apresenta 2 boas práticas para gerir palavras-passe.
- 3.3. O que é o phishing? Como se pode identificar?

4. V/F

- 4.1. Partilhar a localização em tempo real é sempre seguro. (V/F)
- 4.2. A RGPD protege os dados pessoais dos cidadãos europeus. (V/F)
- 4.3. Usar a mesma palavra-passe em todas as contas é recomendado. (V/F)
- 4.4. O phishing pode chegar por e-mail. (V/F)
- 4.5. As redes sociais são sempre seguras para partilhar fotos. (V/F)

Soluções — Privacidade e Dados Pessoais

7.º Ano

TIC

Resolução completa

1. Dados pessoais

- 1.1. Informação que identifica uma pessoa: nome, morada, número de telefone.
- 1.2. Para evitar roubo de identidade, chantagem, uso indevido.
- 1.3. Roubo de identidade; cyberbullying; chantagem.
- 1.4. Regulamento Geral de Proteção de Dados — proteger dados pessoais de cidadãos da UE.

2. Privacidade digital

- 2.1. Configurar privacidade nas redes sociais; usar pseudónimos; limitar partilha de dados.
- 2.2. Quem pode ver as publicações; quem pode contactar; quem pode ver a lista de amigos.
- 2.3. As plataformas atualizam frequentemente; mudanças nas políticas podem expor dados.
- 2.4. Morada completa; número de telefone; rotinas diários.

3. Segurança de contas

- 3.1. Dupla verificação (password + código SMS/app) — adiciona camada extra de segurança.
- 3.2. Usar geradores de palavras-passe; não partilhar palavras-passe; usar gestor de palavras-passe.
- 3.3. Mensagens falsas que imitam entidades fidedignas; verificar remetente, links suspeitos.

4. V/F

- 4.1. Falso — pode comprometer segurança.
- 4.2. Verdadeiro.
- 4.3. Falso — deve usar palavras-passe diferentes.
- 4.4. Verdadeiro.
- 4.5. Falso — devem configurar privacidade.