2025

Tecnologias da Informação e Comunicação

OS EXPLORADORES DIGITAIS – A MISSÃO DO SABER

RUI COSTA

Índice

INTRODUÇÃO 4
O que vais encontrar neste livro? 4
Como usar este livro? 4
CAPÍTULO 1: O DESAFIO DO MICROSOFT TEAMS 5
Um vídeo suspeito 5
"MICROSOFT TEAMS HACKEADO! Descobre como podes ver mensagens secretas!" 5
A Investigação Começa 5
O QUE APRENDEMOS? 6
CAPÍTULO 2: A SENHA INQUEBRÁVEL 7
Uma falha de segurança? 7
O Desafio da Senha 7
Autenticação em Dois Fatores 8
O QUE APRENDEMOS? 8
CAPÍTULO 3: FAKE NEWS OU REALIDADE? 9
Uma notícia chocante 9
Como verificar se uma notícia é verdadeira? 9
Fake news podem ser perigosas 10
O QUE APRENDEMOS? 10
CAPÍTULO 4: WINDOWS VS. LINUX – O DEBATE DIGITAL 11
Qual é o melhor sistema operativo? 11
Windows vs. Linux: quais as diferenças? 11
O QUE APRENDEMOS? 12
CAPÍTULO 5: O VÍRUS INVISÍVEL 12
Um download suspeito 12
O perigo do malware 13
Como nos protegermos contra vírus? 13
O QUE APRENDEMOS? 14

Publicado em março de 2025.

CAPÍTULO 6: PESQUISA NA INTERNET – ENCONTRA A VERDADE! 15
Informações contraditórias 15
Como fazer uma pesquisa eficaz? 15
Como refinar a pesquisa? 16
O QUE APRENDEMOS? 16
CAPÍTULO 7: A IMAGEM MANIPULADA 17
Uma fotografia inacreditável 17
Como verificar se uma imagem foi manipulada? 17
Como fazer uma pesquisa por imagem? 17
O QUE APRENDEMOS? 18
CAPÍTULO 8: O PODER DOS ATALHOS 19
Trabalhar mais rápido no computador 19
Os atalhos mais úteis 19
Como inserir caracteres especiais no teclado português 20
O QUE APRENDEMOS? 21
CAPÍTULO 9: PROTEGE A TUA IDENTIDADE DIGITAL! 22
Partilhar ou não partilhar? 22
O perigo da exposição online 22
Como proteger a identidade digital? 22
O QUE APRENDEMOS? 23
CAPÍTULO 10: CRIAR E EDITAR IMAGENS – A FERRAMENTA CERTA PARA CADA MOMENTO 24
A criação do cartaz 24
Onde encontrar imagens sem violar direitos de autor? 24
Como editar imagens com o GIMP e o Photopea 25
O QUE APRENDEMOS? 25
CAPÍTULO 11: A GRANDE MISSÃO DIGITAL 26
O desafio final 26
O desafio dos exploradores digitais 26

Publicado em março de 2025.

O QUE APRENDEMOS? 27

QUESTÕES DE REFLEXÃO 31

Microsoft Teams 31

Segurança na Internet – Proteção da Identidade e Senhas 31

Mensagens Falsas e Manipuladas (Fake News) 31

Sistemas Operativos – Windows e Linux 32

Utilização de Antivírus e Proteção contra Malware 32

Pesquisa na Internet e Navegadores Web 33

Edição de Imagem – GIMP e Photopea 33

Funções do Teclado e Atalhos Úteis 33

Segurança na Internet – Proteção de Senhas e Identidade Digital 34

Publicado em março de 2025.

INTRODUÇÃO

Bem-vindo a uma aventura digital cheia de mistérios, descobertas e desafios!

Neste livro, vais acompanhar Ana, Tomás, Rafa e Rita, quatro amigos curiosos que adoram tecnologia, mas que nem sempre sabem os perigos e segredos que o mundo digital esconde. Com a ajuda de Mauzão, um cão sábio e cheio de conhecimento, e Tareco, um gato curioso que questiona tudo, vais aprender a navegar na Internet com segurança, a proteger os teus dados e a desenvolver competências digitais essenciais.

O que vais encontrar neste livro?

- **Segurança na Internet** → Como protegeres as tuas contas e identidade digital.
- **Notícias falsas** → Como saber se uma informação é verdadeira ou manipulada.
- **Sistemas operativos** → Windows ou Linux, qual escolher?
- **Vírus e malware** → Como evitar ataques informáticos.
- **Pesquisa na Internet** → Como encontrar a informação certa mais rapidamente.
- **Edição de imagem** → Como editar fotos de forma ética e criativa.
- **Atalhos de teclado** → Como usar o computador de forma mais rápida e eficiente.
- **Direitos de autor** → O que podes ou não usar da Internet.

Mas este **não é um livro qualquer**. Cada capítulo é uma história, com desafios reais que os nossos protagonistas enfrentam no seu dia a dia. Vais rir, aprender e, acima de tudo, tornar-te um verdadeiro **Explorador Digital**!

Como usar este livro?

- **Lê cada capítulo com atenção.** A história vai ajudar-te a perceber como a tecnologia pode ser usada de forma segura e responsável.
- **Reflete sobre as perguntas no final de cada capítulo.** Elas vão ajudar-te a consolidar o que aprendeste.
- **Coloca em prática os conhecimentos adquiridos.** A Internet pode ser um espaço incrível, mas também cheio de desafios. Com este livro, vais estar preparado para enfrentá-los!

Prepara-te para embarcar nesta missão e tornar-te um especialista no mundo digital. **Estás pronto?**

Vem connosco nesta aventura!

Publicado em março de 2025.

CAPÍTULO 1: O DESAFIO DO MICROSOFT TEAMS

Um vídeo suspeito

Ana, Tomás, Rafa e Rita estavam sentados no parque, cada um com o telemóvel na mão. De repente, Rafa abriu os olhos de surpresa.

— Pessoal, vejam isto!

No ecrã, um vídeo do TikTok dizia:

"MICROSOFT TEAMS HACKEADO! Descobre como podes ver mensagens secretas!"

— O quê?! Como é que isso é possível? — perguntou Rita.

— Hmmm... isto parece-me falso. Mas como podemos ter a certeza? — questionou Ana.

— Boa pergunta! Vamos investigar. — disse Tomás.

Mauzão e Tareco estavam deitados na relva, a ouvir tudo.

— A sério?! Outra fake news a espalhar-se? Como é que eles ainda acreditam nestas coisas? — disse Mauzão, revirando os olhos.

— Mas... e se for verdade, Mauzão? Já pensaste? Se calhar, há mesmo mensagens secretas no Teams! — questionou Tareco.

— Ai, Tareco... És tão ingénuo. Vamos ver o que eles descobrem.

A Investigação Começa

Os amigos decidiram testar a informação. Se fosse verdade, tinham de encontrar provas.

1. **Entraram no Microsoft Teams e procuraram mensagens secretas.**
   Resultado: Nada. Tudo estava normal.
2. **Pesquisaram no Google: "Microsoft Teams hackeado 2024".**
   Resultado: Nenhuma notícia verdadeira sobre o assunto.
3. **Usaram sites de fact-checking, como o Polígrafo.**
   Resultado: O vídeo era uma fake news.

— Uau! Então o vídeo era falso? — perguntou Tareco.

— Óbvio! Nunca deves acreditar logo no que vês na Internet. — respondeu Mauzão.

— Mas como é que os humanos podem saber o que é verdade ou mentira?

— Fácil! Há três regras de ouro:

1. Verificar a fonte da informação.
2. Pesquisar noutros sites confiáveis.
3. Usar fact-checkers, como o Polígrafo ou o Snopes.

— Hmmm... Então nem tudo o que aparece na Internet é verdade?

— Exato, Tareco! Se fosse assim, já teríamos gatos a governar o mundo.

— E isso seria assim tão mau porquê?!

— Ai, ai...

O QUE APRENDEMOS?

- O Microsoft Teams não foi hackeado. A notícia era falsa.
- Nunca devemos acreditar em tudo o que vemos online.
- Devemos sempre verificar fontes e usar fact-checkers.

E tu? Já viste alguma notícia estranha na Internet? Como podes verificar se é verdadeira?

Continua no próximo capítulo...

CAPÍTULO 2: A SENHA INQUEBRÁVEL

Uma falha de segurança?

Na manhã seguinte, Ana, Tomás, Rafa e Rita estavam na biblioteca da escola a trabalhar num projeto.

— Viram o que aconteceu ontem? — perguntou Tomás. — Uma empresa gigante foi hackeada porque os funcionários usavam senhas fracas.

— Como assim? — perguntou Rita.

— Alguém conseguiu entrar no sistema porque muitas pessoas usavam senhas como "123456" ou "password".

— Mas quem é que ainda usa senhas assim?! — exclamou Ana.

Mauzão e Tareco estavam sentados ao lado dos alunos, fingindo estar distraídos, mas a ouvir tudo atentamente.

— A sério, Tareco? Ainda há humanos que usam "123456" como senha? — perguntou Mauzão.

— Talvez seja fácil de lembrar... — respondeu Tareco.

— Sim, e também é fácil de adivinhar! Uma senha fraca é como uma porta aberta para os hackers.

— Então como se cria uma senha segura? — perguntou Tareco.

— Vamos ver se os humanos descobrem.

O Desafio da Senha

Os amigos decidiram testar o que tinham aprendido.

1. **Criaram uma senha com o nome de cada um.**
   Resultado: O sistema disse que era "fraca".
2. **Adicionaram números.**
   Resultado: Ainda era considerada "média".
3. **Juntaram símbolos e tornaram-na mais longa.**
   Resultado: Agora era "muito forte"!

— Parece que quanto mais variada for a senha, mais difícil é de adivinhar! — disse Rita.

— Exatamente! — concordou Tomás. — E devemos ter uma senha diferente para cada conta.

— Mas como é que alguém pode lembrar-se de tantas senhas? — perguntou Rafa.

— Podemos usar um gestor de senhas. Ele guarda tudo por nós e só precisamos de lembrar uma senha principal.

Mauzão olhou para Tareco com um ar de satisfação.

— Vês, Tareco? Criar uma senha segura não é assim tão difícil.

— Mas... e se alguém descobrir a senha? — perguntou Tareco.

— Ah! Para isso há uma solução ainda melhor! — respondeu Mauzão.

Autenticação em Dois Fatores

Os amigos descobriram que, mesmo com uma senha forte, **há uma camada extra de proteção**: a **Autenticação em Dois Fatores (2FA)**.

— O que é isso? — perguntou Rita.

— É um sistema que pede um código extra quando fazemos login — explicou Ana. — Mesmo que alguém descubra a nossa senha, não consegue entrar sem esse código.

— Como quando recebemos um SMS com um código ao fazer login nalguns sites? — perguntou Rafa.

— Exatamente! — confirmou Tomás.

Mauzão abanou a cauda.

— Finalmente, estão a perceber! A 2FA é como uma fechadura extra na porta.

— Então devemos ativar a 2FA em todas as contas? — perguntou Tareco.

— Sempre que possível. Assim, as contas ficam mais protegidas.

O QUE APRENDEMOS?

- As senhas fracas podem ser facilmente descobertas por hackers.
- Para criar uma senha segura, devemos misturar letras maiúsculas, minúsculas, números e símbolos.
- Nunca devemos usar a mesma senha em diferentes contas.
- Um gestor de senhas pode ajudar a guardar todas as nossas senhas.
- A Autenticação em Dois Fatores (2FA) adiciona uma camada extra de segurança.

E tu? As tuas senhas são seguras? Já ativaste a 2FA nas tuas contas?

Continua no próximo capítulo...

Publicado em março de 2025.

CAPÍTULO 3: FAKE NEWS OU REALIDADE?

Uma notícia chocante

Ana, Tomás, Rafa e Rita estavam sentados na esplanada quando o telemóvel de Rafa apitou.

— Vejam isto! — exclamou Rafa. — Acabei de receber uma notícia no grupo da família a dizer que um YouTuber famoso foi preso!

— O quê?! — perguntou Rita. — Ele lançou um vídeo ontem, como é que isso é possível?

— Parece estranho... — disse Ana. — Onde encontraste essa notícia?

— No WhatsApp. Foi o meu tio que enviou.

Tomás franziu a testa.

— Então vamos verificar se é verdade.

Mauzão e Tareco estavam sentados perto do grupo, atentos à conversa.

— Lá vamos nós outra vez... — suspirou Mauzão.

— Mas pode ser verdade! — disse Tareco. — Se toda a gente está a partilhar, deve ser real!

— Tareco, partilhar muito não significa que seja verdade. Vamos ver se eles aprendem a verificar a informação.

Como verificar se uma notícia é verdadeira?

Os amigos decidiram investigar.

1. **Pesquisaram o título da notícia no Google.**
   Resultado: Nenhum site confiável falava sobre o assunto.
2. **Foram a sites de fact-checking, como o Polígrafo.**
   Resultado: Era uma fake news.
3. **Verificaram a fonte da notícia.**
   Resultado: Era um site desconhecido, sem data nem autor.

— Isto é falso! — disse Tomás.

— Mas parecia tão real... — comentou Rita.

— É por isso que devemos sempre confirmar antes de partilhar. — explicou Ana.

Mauzão abanou as orelhas.

— Finalmente, alguém que pensa antes de espalhar mentiras!

Tareco inclinou a cabeça.

— Mas porque é que alguém inventaria uma notícia falsa?

— Por vários motivos. Alguns querem enganar as pessoas, outros querem cliques e dinheiro. E há quem queira só confundir os leitores.

— Então, como podemos saber se uma notícia é verdadeira?

— Com três passos simples:

1. **Verificar a fonte.** O site é confiável? Tem um autor identificado?
2. **Comparar com outros sites.** Se for verdade, outros meios de comunicação também vão falar sobre isso.
3. **Usar um site de fact-checking.** Como o Polígrafo ou o Snopes.

Fake news podem ser perigosas

— Partilhar fake news pode causar muitos problemas. — disse Rita. — Algumas fazem as pessoas ter medo sem razão. Outras podem prejudicar a reputação de alguém.

— Exato! — concordou Ana. — E algumas até podem ser usadas para enganar pessoas e roubar dinheiro.

— Como aqueles emails falsos a dizer que ganhámos um prémio? — perguntou Rafa.

— Sim! Chamamos isso de phishing. Mas vamos falar sobre isso noutro dia.

Mauzão sorriu.

— Estes humanos estão a aprender depressa.

— Sim, mas agora fiquei com uma dúvida. — disse Tareco. — Se uma notícia falsa for muito bem escrita, como é que sabemos que é mentira?

— É por isso que devemos sempre investigar antes de acreditar.

— Acho que vou passar a verificar tudo.

— Finalmente, Tareco! Acho que estás a ficar esperto.

O QUE APRENDEMOS?

- Nem tudo o que vemos na Internet é verdade.
- Antes de partilhar, devemos sempre verificar a fonte, comparar com outros sites e usar fact-checkers.
- Fake news podem causar problemas e prejudicar pessoas.
- Algumas notícias falsas são criadas para enganar ou para ganhar dinheiro.
- Devemos sempre pensar antes de partilhar uma informação.

E tu? Já viste alguma fake news? Como podes verificar se uma notícia é verdadeira?

Continua no próximo capítulo...

Publicado em março de 2025.

CAPÍTULO 4: WINDOWS VS. LINUX – O DEBATE DIGITAL

Qual é o melhor sistema operativo?

Era hora de almoço e Ana, Tomás, Rafa e Rita estavam na biblioteca. Tomás, como sempre, estava no computador.

— O que estás a fazer? — perguntou Rita.

— Estou a instalar o Linux neste computador antigo. — respondeu Tomás.

— O Linux? Mas para que serve isso? — perguntou Rafa. — Toda a gente usa Windows!

— Nem toda a gente. — disse Tomás. — Sabiam que muitos programadores e empresas usam Linux porque é gratuito e mais seguro?

— Mas o Windows é mais fácil de usar! — argumentou Ana.

— Depende do que precisas. Cada sistema tem vantagens e desvantagens.

Mauzão e Tareco estavam ao lado dos alunos, como sempre, a ouvir tudo.

— Ah, este debate nunca acaba... — suspirou Mauzão.

— Mas qual dos dois é melhor, afinal? — perguntou Tareco.

— Isso depende. Vamos ouvir os humanos.

Windows vs. Linux: quais as diferenças?

Os amigos decidiram fazer uma lista com as características dos dois sistemas operativos.

Windows:

✓ Fácil de usar, ideal para quem está habituado a computadores.

✓ Compatível com a maioria dos programas e jogos.

✓ Suporte oficial da Microsoft.

✗ Pago, precisa de uma licença.

✗ Pode ser mais vulnerável a vírus.

Linux:

✓ Gratuito e de código aberto.

✓ Mais seguro, com menos vírus.

✓ Melhor para programadores e servidores.

✗ Pode ser mais difícil para quem nunca usou.

✗ Alguns programas populares não funcionam.

— Então, Linux ou Windows? — perguntou Rita.

— Depende do que cada um precisa. — disse Ana.

— Exatamente! — concordou Tomás. — Se quiseres jogar e usar programas comuns, Windows pode ser melhor. Se quiseres algo mais seguro e grátis, Linux é uma ótima opção.

Tareco coçou a cabeça.

— Então... Linux é melhor ou não?

— Para algumas coisas, sim. Para outras, não. O melhor sistema é aquele que funciona melhor para cada pessoa.

— Isso faz sentido!

Mauzão sorriu.

— Vês, Tareco? O mundo da tecnologia não é preto e branco. Há sempre vantagens e desvantagens.

O QUE APRENDEMOS?

- Windows e Linux são dois sistemas operativos diferentes, cada um com as suas vantagens e desvantagens.
- O Windows é mais fácil de usar e compatível com mais programas, mas é pago e mais vulnerável a vírus.
- O Linux é gratuito e mais seguro, mas pode ser mais difícil para principiantes.
- O melhor sistema operativo depende das necessidades do utilizador.

E tu? Já experimentaste Linux? Qual sistema operativo preferes?

Continua no próximo capítulo...

CAPÍTULO 5: O VÍRUS INVISÍVEL

Um download suspeito

Ana, Tomás, Rafa e Rita estavam sentados no jardim da escola, cada um com o seu telemóvel ou computador. De repente, Rafa mostrou um site aos amigos.

— Vejam isto! Um site onde podemos descarregar jogos pagos de graça!

— Isso parece suspeito... — disse Ana.

— Mas parece verdadeiro! O site tem um design profissional e até tem comentários positivos! — insistiu Rafa.

— Devíamos ter cuidado. Muitos sites assim escondem vírus. — alertou Tomás.

Mauzão e Tareco estavam a observar tudo, atentos ao que ia acontecer.

— Aqui vamos nós outra vez... — suspirou Mauzão.

— Mas e se o site for mesmo seguro? — perguntou Tareco.

— Não existe "jogos pagos de graça" assim tão facilmente. Isso é um truque clássico para espalhar vírus. Vamos ver se os humanos percebem.

O perigo do malware

Tomás decidiu fazer um teste. Criou um ambiente seguro no seu computador e descarregou um dos jogos. Assim que abriu o ficheiro, o antivírus deu um alerta vermelho: **"Ameaça detetada: Malware encontrado!"**

— Sabia! — exclamou Tomás.

— O que aconteceu? — perguntou Rita.

— O ficheiro parecia um jogo, mas na verdade tinha um vírus escondido!

Os amigos começaram a pesquisar e descobriram que há vários tipos de malware:

- **Vírus** – Programas que se espalham e danificam ficheiros.
- **Spyware** – Espia o que fazemos no computador.
- **Ransomware** – Bloqueia os ficheiros e pede dinheiro para os devolver.

— Então, se tivéssemos instalado este jogo, podíamos ter sido atacados por um vírus? — perguntou Rafa.

— Sim! E, em alguns casos, os hackers podem roubar os nossos dados ou bloquear o computador.

Tareco arregalou os olhos.

— Uau! Eu achava que vírus era só para deixar o computador lento!

— Não, Tareco. O malware pode roubar informação, espiar utilizadores e até pedir dinheiro.

— Então como podemos evitar isto?

Como nos protegermos contra vírus?

Os amigos fizeram uma lista com dicas para evitar malware:

1. **Ter um antivírus atualizado** – Ele avisa quando há ameaças.
2. **Evitar downloads de sites desconhecidos** – Muitos escondem vírus.
3. **Nunca abrir anexos suspeitos em emails** – Podem conter malware.

4. **Manter o sistema e os programas atualizados** – Atualizações corrigem falhas de segurança.
5. **Fazer backup dos ficheiros importantes** – Para não perder dados caso algo corra mal.

— Então, foi uma sorte termos verificado antes de instalar o jogo! — disse Ana.

— Exatamente! — respondeu Tomás.

Mauzão sorriu satisfeito.

— Finalmente, os humanos aprenderam algo útil.

— Sim... Mas Rafa ainda queria o jogo grátis. — disse Tareco.

— Paciência, Tareco. Às vezes, o que parece bom demais para ser verdade... é mesmo mentira.

O QUE APRENDEMOS?

- Alguns sites oferecem downloads falsos para espalhar vírus.
- Malware pode danificar o computador, roubar dados ou pedir dinheiro para desbloquear ficheiros.
- Devemos sempre usar antivírus e evitar instalar ficheiros suspeitos.
- Nunca devemos abrir anexos de emails desconhecidos.
- Fazer backup dos ficheiros ajuda a prevenir perdas.

E tu? Já recebeste algum alerta de antivírus? Como te proteges online?

Continua no próximo capítulo...

CAPÍTULO 6: PESQUISA NA INTERNET – ENCONTRA A VERDADE!

Informações contraditórias

Ana, Tomás, Rafa e Rita estavam a fazer um trabalho para a escola sobre energias renováveis.

— Já tenho informação! — disse Rafa, entusiasmado. — Encontrei um site que diz que a energia solar é a melhor opção para o futuro.

— Mas este outro site diz que a energia eólica é muito mais eficiente. — respondeu Rita.

— E eu encontrei um artigo a dizer que nenhuma dessas energias é viável. — acrescentou Tomás.

Ana franziu a testa.

— Então qual delas está certa?

Mauzão e Tareco, que estavam sentados perto dos alunos, ouviam com atenção.

— Este é um problema clássico, Tareco. Nem todas as informações na Internet são fiáveis.

— Mas como é que sabemos em quem confiar?

— Vamos ver se os humanos descobrem.

Como fazer uma pesquisa eficaz?

Os amigos decidiram testar algumas estratégias para encontrar informações fiáveis.

1. **Usaram palavras-chave específicas.**
   Resultado: Os motores de busca mostraram sites mais relevantes.
2. **Compararam diferentes fontes.**
   Resultado: Alguns sites tinham opiniões em vez de factos.
3. **Verificaram a credibilidade dos sites.**
   Resultado: Descobriram que alguns artigos eram patrocinados por empresas interessadas em vender produtos.

— Então, a primeira coisa a fazer é verificar se o site é confiável. — disse Ana.

— E nunca acreditar apenas num único site. — acrescentou Tomás.

— Exato! Devemos comparar várias fontes antes de chegarmos a uma conclusão.

Tareco parecia confuso.

— Mas como é que sabemos se um site é confiável?

— Existem alguns sinais:

1. **Terminação do site:** Sites terminados em **.edu**, **.gov** ou **.org** costumam ser mais fiáveis.
2. **Autor identificado:** O artigo tem um autor ou especialista na área?
3. **Fontes e referências:** Um bom artigo menciona onde encontrou a informação.
4. **Data de publicação:** Informação antiga pode estar desatualizada.

Como refinar a pesquisa?

— Há outra coisa que podemos fazer: usar **operadores de pesquisa** para encontrar resultados mais exatos. — disse Tomás.

— Operadores de pesquisa? O que é isso? — perguntou Rafa.

— São comandos especiais que ajudam a encontrar o que procuramos mais rapidamente.

Os amigos fizeram uma lista de operadores úteis:

- **Aspas ("")** → Procura a frase exata (exemplo: "energia solar vantagens").
- **Sinal de menos (-)** → Exclui palavras da pesquisa (exemplo: carros elétricos -Tesla).
- **site:** → Pesquisa dentro de um site específico (exemplo: energia solar site:bbc.com).
- **filetype:** → Procura um tipo de ficheiro específico (exemplo: energia solar filetype:pdf).

— Com estas técnicas, conseguimos encontrar informação mais precisa e fiável. — concluiu Ana.

Tareco abanou a cauda.

— Afinal, pesquisar na Internet é mais complicado do que eu pensava.

— Não é complicado, Tareco. Só exige paciência e atenção. — respondeu Mauzão.

— Ainda bem que agora sei como encontrar a verdade!

O QUE APRENDEMOS?

- Nem todas as informações na Internet são fiáveis.
- Devemos comparar várias fontes antes de acreditar numa informação.
- Sites com terminações **.edu**, **.gov** e **.org** costumam ser mais confiáveis.
- Devemos verificar o autor, as fontes e a data de publicação.
- Os operadores de pesquisa ajudam a encontrar resultados mais específicos.

E tu? Já encontraste informações contraditórias na Internet? Como verificaste qual era verdadeira?

Continua no próximo capítulo...

CAPÍTULO 7: A IMAGEM MANIPULADA

Uma fotografia inacreditável

Ana, Tomás, Rafa e Rita estavam sentados num café quando Rita abriu o Instagram e arregalou os olhos.

— Pessoal, vejam isto! — disse, mostrando uma fotografia.

Era uma imagem de um animal estranho, uma mistura de lobo e tigre, com olhos brilhantes.

— Nunca vi nada assim! — exclamou Rafa.

— Parece um animal extinto que voltou à vida! — disse Tomás.

— Mas será que é real? — perguntou Ana.

Mauzão e Tareco espreitaram o ecrã do telemóvel de Rita.

— Lá vamos nós outra vez... — suspirou Mauzão.

— Mas... e se for verdade? — perguntou Tareco.

— Se parece bom demais para ser verdade, provavelmente não é. Vamos ver se os humanos percebem isso.

Como verificar se uma imagem foi manipulada?

Os amigos decidiram investigar.

1. **Pesquisaram o nome do animal no Google.**
   Resultado: Não havia registos científicos sobre ele.
2. **Fizeram uma pesquisa por imagem reversa.**
   Resultado: Descobriram que a imagem original era de um lobo, mas alguém a tinha editado.
3. **Analisaram detalhes da imagem.**
   Resultado: As sombras e texturas não eram naturais.

— Isto foi editado! — concluiu Tomás.

— Então não é real? — perguntou Rita.

— Não. Alguém alterou a imagem para enganar as pessoas ou apenas por diversão.

— Como é que fizemos essa pesquisa por imagem reversa? — perguntou Rafa.

Como fazer uma pesquisa por imagem?

Os amigos aprenderam que há várias formas de verificar se uma imagem é verdadeira:

1. **Usar o Google Lens ou o TinEye.**
2. **Procurar detalhes estranhos na imagem.** Muitas edições falham nas sombras e reflexos.
3. **Verificar a fonte.** Foi publicado num site confiável ou numa rede social desconhecida?
4. **Comparar com outras imagens.** Se for real, haverá mais fotos tiradas de ângulos diferentes.

— Então, da próxima vez que virmos algo incrível na Internet, devemos sempre verificar antes de acreditar. — disse Ana.

Mauzão sorriu.

— Finalmente, os humanos aprenderam algo útil.

Tareco abanou a cauda.

— Já percebi! Algumas imagens são falsas, mas parecem tão reais que é fácil sermos enganados.

— Exatamente, Tareco. E quanto mais as pessoas partilham sem verificar, mais a mentira se espalha.

O QUE APRENDEMOS?

- Nem todas as imagens que vemos na Internet são reais.
- Podemos verificar imagens usando pesquisa reversa no Google Lens ou TinEye.
- As sombras, texturas e reflexos podem revelar manipulações.
- Devemos sempre verificar a fonte antes de partilhar.

E tu? Já viste alguma imagem falsa na Internet? Como podes verificar se é verdadeira?

Continua no próximo capítulo...

CAPÍTULO 8: O PODER DOS ATALHOS

Trabalhar mais rápido no computador

Ana, Tomás, Rafa e Rita estavam na biblioteca a terminar um trabalho de grupo. Ana estava a escrever no computador quando, de repente, tudo desapareceu.

— O quê?! Onde foi parar o meu texto?! — exclamou Ana.

— Carrega em Ctrl + Z! — disse Tomás.

Ana seguiu o conselho e, como por magia, o texto voltou.

— Uau! Como é que fizeste isso? — perguntou Rafa.

— Atalhos de teclado! Ctrl + Z desfaz a última ação. — explicou Tomás.

Mauzão e Tareco estavam deitados perto do grupo, atentos.

— Estes humanos deviam aprender mais atalhos, Tareco. — disse Mauzão.

— Mas eles já sabem usar o rato! Para que precisam de atalhos? — perguntou Tareco.

— Porque assim trabalham mais rápido. Vamos ver se percebem.

Os atalhos mais úteis

Os amigos decidiram aprender mais atalhos para facilitar o trabalho.

1. **Ctrl + C e Ctrl + V** → Copiar e colar.
2. **Ctrl + X** → Cortar.
3. **Ctrl + Z** → Desfazer a última ação.
4. **Ctrl + S** → Guardar rapidamente um ficheiro.
5. **Alt + Tab** → Alternar entre programas abertos.
6. **Ctrl + P** → Imprimir um documento.
7. **Windows + D** → Minimizar todas as janelas e mostrar o ambiente de trabalho.
8. **Ctrl + F** → Pesquisar uma palavra numa página ou documento.

— Então podemos fazer tudo mais rápido sem precisar de andar sempre com o rato! — concluiu Rita.

— Exatamente! — disse Tomás.

Tareco arregalou os olhos.

— Parece magia! Acho que vou decorar estes atalhos!

— Não é magia, Tareco. É eficiência. — respondeu Mauzão.

— Mas e se eu quiser escrever um carácter especial, como um acento ou símbolo? — perguntou Tareco.

— Também há atalhos para isso! — respondeu Mauzão.

Como inserir caracteres especiais no teclado português

Os amigos descobriram que podiam usar combinações de teclas para escrever letras com acentos e símbolos essenciais:

Acentos e letras especiais

1. **´ + a, e, i, o, u** → á, é, í, ó, ú
2. **` + a, e, i, o, u** → à, è, ì, ò, ù
3. **^ + a, e, i, o, u** → â, ê, î, ô, û
4. **~ + a, o, n** → ã, õ, ñ
5. **Ç** → Tecla direta no teclado português

Símbolos mais usados

1. **Alt Gr + 2** → @
2. **Alt Gr + E** → €
3. **Shift + 1** → !
4. **Shift + 2** → "
5. **Shift + 3** → #
6. **Shift + 4** → $
7. **Shift + 5** → %
8. **Shift + 6** → &
9. **Shift + 7** → /
10. **Shift + 8** → (
11. **Shift + 9** →)
12. **Shift + 0** → =

— Agora já não precisamos de procurar símbolos no teclado! — disse Ana.

— Se aprendermos estes atalhos, vamos poupar muito tempo. — concordou Rafa.

Mauzão abanou a cauda, satisfeito.

— Missão cumprida!

Tareco sorriu.

— Já sei como impressionar os outros gatos! Vou escrever mensagens super-rápidas!

O QUE APRENDEMOS?

- Os atalhos de teclado ajudam a trabalhar mais rápido.
- Podemos copiar, colar e desfazer ações sem usar o rato.
- Existem atalhos para alternar entre programas e pesquisar palavras.
- Podemos usar combinações de teclas para escrever caracteres especiais.

E tu? Já usaste algum atalho de teclado? Qual é o teu favorito?

Continua no próximo capítulo...

CAPÍTULO 9: PROTEGE A TUA IDENTIDADE DIGITAL!

Partilhar ou não partilhar?

Ana, Tomás, Rafa e Rita estavam sentados na esplanada, a lanchar. Rafa estava a ver as redes sociais quando sorriu.

— Olhem esta foto da minha prima na escola! Vou partilhar nos meus stories.

— Tens a certeza de que ela quer que publiques isso? — perguntou Ana.

— Claro! É só uma foto, não tem mal.

— Mas estás a mostrar onde ela estuda... — alertou Tomás.

Mauzão e Tareco, que estavam sentados ao lado do grupo, prestaram atenção à conversa.

— Aqui vamos nós outra vez... — suspirou Mauzão.

— Mas qual é o problema de publicar uma foto? Toda a gente o faz! — disse Tareco.

— Exatamente por isso é que devemos ter cuidado. Vamos ver se os humanos percebem o perigo.

O perigo da exposição online

Os amigos começaram a pensar melhor sobre o que publicam na Internet.

1. **Fotos com localização visível** podem dar pistas sobre onde estudam ou vivem.
2. **Publicações com horários regulares** podem mostrar a rotina de alguém.
3. **Informação pessoal (telefone, email, morada)** pode ser usada por desconhecidos.
4. **Perfis públicos permitem que qualquer pessoa veja as publicações.**

— Então se eu publicar muitas fotos na escola, alguém pode descobrir onde estudo e quando estou lá? — perguntou Rita.

— Exato! — confirmou Ana. — E se fores a um café todos os dias à mesma hora e publicares sempre uma foto, alguém pode perceber o teu horário.

Tareco arregalou os olhos.

— Isso é assustador!

— É por isso que devemos ter cuidado com o que partilhamos.

Como proteger a identidade digital?

Para evitar problemas, os amigos decidiram seguir algumas regras:

1. **Privacidade das redes sociais** – Tornar o perfil privado e aprovar seguidores.

2. **Evitar partilhar informação pessoal** – Nome completo, morada e contactos devem ser mantidos em segurança.
3. **Rever as configurações de segurança** – Controlar quem pode ver as publicações.
4. **Usar senhas fortes e autenticação em dois fatores** – Para proteger as contas contra invasões.
5. **Pensar antes de publicar** – Perguntar: "Isto pode ser usado contra mim?"

— A partir de agora, só vou partilhar fotos com a permissão das pessoas que aparecem nelas. — disse Rafa.

— E vou rever as minhas definições de privacidade! — acrescentou Rita.

Mauzão sorriu.

— Missão cumprida!

Tareco suspirou.

— Isto significa que não posso mais publicar fotos da minha comida?

— Podes, Tareco. Mas lembra-te: na Internet, tudo o que publicas pode ser visto por mais pessoas do que imaginas.

O QUE APRENDEMOS?

- Devemos ter cuidado com as informações que partilhamos online.
- Perfis privados são mais seguros do que perfis públicos.
- Publicar fotos e rotinas pode expor demasiado a nossa vida.
- As configurações de segurança das redes sociais devem ser revistas regularmente.
- Antes de publicar algo, devemos pensar se pode ser usado contra nós.

E tu? Já verificaste as tuas definições de privacidade nas redes sociais?

Continua no próximo capítulo...

CAPÍTULO 10: CRIAR E EDITAR IMAGENS – A FERRAMENTA CERTA PARA CADA MOMENTO

A criação do cartaz

Ana, Tomás, Rafa e Rita estavam na biblioteca, a trabalhar num cartaz para uma campanha da escola.

— Precisamos de uma imagem impactante para o nosso cartaz. — disse Rita.

— Podemos procurar no Google! — sugeriu Rafa.

— Cuidado! Nem todas as imagens podem ser usadas livremente. Algumas têm direitos de autor. — alertou Ana.

Mauzão e Tareco estavam atentos.

— Aqui está um erro comum, Tareco. Muitos humanos usam imagens sem pensar se podem ou não.

— Então como sabem quais podem usar? — perguntou Tareco.

— Vamos ver se eles descobrem.

Onde encontrar imagens sem violar direitos de autor?

Os amigos pesquisaram formas seguras de obter imagens:

1. **Bancos de imagens gratuitas** → Unsplash, Pixabay, Pexels.
2. **Filtros do Google Imagens** → Opção "Direitos de utilização" > "Licenças Creative Commons".
3. **Criar as suas próprias imagens** → Usar um editor para personalizar gráficos.

— Então não podemos simplesmente copiar qualquer imagem da Internet? — perguntou Rafa.

— Não! Algumas imagens pertencem a fotógrafos ou designers, e é ilegal usá-las sem permissão. — explicou Ana.

— Certo! Vou sempre procurar imagens em bancos gratuitos ou verificar a licença antes de usar. — disse Tomás.

Mauzão sorriu.

— Boa decisão! Mas agora falta aprender a editá-las.

Como editar imagens com o GIMP e o Photopea

Os amigos decidiram personalizar uma imagem para o cartaz. Para isso, usaram dois editores gratuitos:

- **GIMP** (instalado no computador)
- **Photopea** (funciona online, sem precisar de instalar)

Os amigos aprenderam algumas funções básicas:

1. **Recortar e redimensionar** → Para ajustar imagens ao tamanho certo.
2. **Corrigir cores e brilho** → Para melhorar a qualidade da imagem.
3. **Remover fundos** → Para criar imagens com fundo transparente.
4. **Adicionar texto e camadas** → Para personalizar cartazes e apresentações.

— Isto é incrível! Agora posso criar os meus próprios designs! — disse Rita.

— E sem precisar de pagar por programas caros. — acrescentou Tomás.

Tareco inclinou a cabeça.

— E se alguém editar uma imagem só para enganar as pessoas?

Mauzão suspirou.

— Isso acontece muito, Tareco. É por isso que no Capítulo 7 aprendemos a verificar imagens falsas. Agora, estamos a aprender a editar de forma ética e criativa.

Tareco sorriu.

— Já percebi! Editar imagens pode ser útil, mas devemos garantir que usamos fontes seguras e respeitamos os direitos de autor!

O QUE APRENDEMOS?

- Nem todas as imagens na Internet podem ser usadas livremente.
- Podemos encontrar imagens gratuitas em bancos de imagens ou usar filtros de pesquisa.
- O GIMP e o Photopea são ferramentas gratuitas para editar imagens.
- Podemos melhorar fotos, criar cartazes e remover fundos com edição de imagem.
- Devemos usar a edição de imagem de forma ética e criativa.

E tu? Já experimentaste editar imagens? Como podes garantir que usas imagens de forma correta e responsável?

Continua no próximo capítulo...

CAPÍTULO 11: A GRANDE MISSÃO DIGITAL

O desafio final

Ana, Tomás, Rafa e Rita estavam sentados no jardim da escola, a relembrar tudo o que tinham aprendido ao longo das últimas semanas.

— Já repararam como agora somos muito mais cuidadosos na Internet? — disse Ana.

— Sim! Antes, eu acreditava em todas as notícias que via online. Agora, já sei como verificar se são verdadeiras! — respondeu Rafa.

— E eu deixei de descarregar ficheiros suspeitos. Não quero que o meu computador apanhe vírus! — acrescentou Rita.

— Eu até comecei a usar senhas mais seguras e a ativar a autenticação em dois fatores. — disse Tomás.

Mauzão e Tareco estavam sentados perto do grupo, satisfeitos com a evolução dos humanos.

— Parece que finalmente aprenderam a proteger-se no mundo digital. — disse Mauzão.

— Mas será que estão mesmo preparados? — perguntou Tareco. — E se fizéssemos um teste?

O desafio dos exploradores digitais

Mauzão e Tareco decidiram lançar um **desafio final** aos amigos. Cada um teria de responder corretamente a algumas perguntas para provar que estava pronto para navegar na Internet com segurança.

1. **Como podemos saber se uma notícia é verdadeira?**

   Verificamos a fonte, comparamos com outros sites e usamos fact-checkers.
2. **Como devemos criar uma senha segura?**

   Deve ser longa e incluir letras maiúsculas, minúsculas, números e símbolos.
3. **Como podemos proteger os nossos dispositivos contra vírus?**

   Instalamos um antivírus, evitamos sites suspeitos e não abrimos anexos de emails desconhecidos.
4. **O que devemos fazer antes de publicar algo nas redes sociais?**

   Pensar se pode ser usado contra nós e verificar as definições de privacidade.
5. **Porque devemos usar a autenticação em dois fatores (2FA)?**

   Porque adiciona uma camada extra de segurança, mesmo que alguém descubra a nossa senha.

6. **Como podemos saber se uma imagem foi manipulada?**
   Usamos pesquisa reversa, verificamos sombras e texturas e comparamos com outras fontes.
7. **Onde podemos encontrar imagens para usar legalmente?**
   Em bancos de imagens gratuitas ou usando filtros de direitos de autor no Google.
8. **Quais são os melhores programas gratuitos para editar imagens?**
   GIMP e Photopea.

Ana, Tomás, Rafa e Rita responderam corretamente a todas as perguntas.

— Parabéns! Agora são verdadeiros exploradores digitais! — disse Mauzão.

— Isso significa que nunca mais vamos cometer erros online? — perguntou Rita.

— Significa que agora sabem como pensar antes de agir. A tecnologia é incrível, mas deve ser usada com inteligência e segurança. — respondeu Mauzão.

Tareco sorriu.

— E já agora, podem ensinar estas regras a mais pessoas. Quanto mais gente souber como estar segura na Internet, melhor!

Ana olhou para os amigos.

— Boa ideia, Tareco! Vamos partilhar este conhecimento na escola. Assim, todos podem aprender a usar a Internet de forma segura!

E assim, os quatro amigos embarcaram na sua maior missão: **ajudar outros a tornarem-se exploradores digitais responsáveis!**

O QUE APRENDEMOS?

- Devemos sempre verificar a veracidade das notícias antes de acreditar nelas.
- As senhas devem ser fortes e diferentes para cada conta.
- Os antivírus e boas práticas evitam ataques informáticos.
- Nunca devemos partilhar informação pessoal sem pensar nas consequências.
- A autenticação em dois fatores torna as contas mais seguras.
- O conhecimento sobre segurança digital deve ser partilhado para ajudar outras pessoas.

E tu? Estás pronto para te tornares um explorador digital responsável?

FIM DA MISSÃO!

Publicado em março de 2025.

GLOSSÁRIO

Aqui encontras os principais termos que aprendeste ao longo desta aventura digital. Se alguma palavra te parecer complicada, consulta esta lista para esclarecer todas as tuas dúvidas!

A

- **Antivírus** – Programa que deteta e remove vírus e malware do computador.
- **Atalhos de teclado** – Combinações de teclas que permitem executar ações rapidamente no computador (exemplo: **Ctrl + C** para copiar).
- **Autenticação em dois fatores (2FA)** – Método de segurança que adiciona uma camada extra de proteção às contas online, exigindo um segundo código além da senha.

B

- **Backup** – Cópia de segurança de ficheiros e dados importantes para evitar perdas.
- **Browser (Navegador)** – Programa usado para aceder à Internet (exemplo: Google Chrome, Mozilla Firefox, Microsoft Edge).

C

- **Creative Commons (CC)** – Tipo de licença que permite usar e partilhar conteúdos, como imagens e vídeos, de forma legal, de acordo com certas condições.
- **Cibersegurança** – Conjunto de práticas e ferramentas que ajudam a proteger computadores, redes e dados de ataques e acessos não autorizados.

D

- **Dados pessoais** – Informação que identifica uma pessoa, como nome, morada, número de telefone ou email.
- **Direitos de autor** – Regras que protegem os criadores de conteúdos, impedindo que o seu trabalho seja copiado sem permissão.

E

- **Edição de imagem** – Processo de alterar ou melhorar imagens com ferramentas digitais como o GIMP ou Photopea.
- **Engenharia social** – Técnica usada por hackers para enganar pessoas e obter informação confidencial, como senhas.

F

- **Fake news (Notícias falsas)** – Informação enganosa ou manipulada que se espalha na Internet como se fosse verdadeira.
- **Fact-checking** – Processo de verificar a veracidade de uma informação, comparando-a com fontes confiáveis.

- **Firewall** – Sistema de segurança que bloqueia acessos não autorizados a um computador ou rede.

G

- **GIMP** – Programa gratuito de edição de imagem, usado para manipular fotos e gráficos.
- **Google Lens** – Ferramenta da Google que permite pesquisar por imagens, identificando objetos, locais e textos nelas contidos.

I

- **Identidade digital** – Conjunto de informações que uma pessoa tem na Internet, incluindo perfis em redes sociais e contas online.
- **Imagem manipulada** – Imagem alterada digitalmente para enganar ou modificar a realidade.
- **Informação falsa** – Conteúdo que apresenta dados errados ou manipulados para enganar os utilizadores.

L

- **Licença Creative Commons** – Tipo de licença que permite o uso gratuito de conteúdos digitais, com certas condições.
- **Linux** – Sistema operativo gratuito e de código aberto, usado em computadores e servidores.

M

- **Malware** – Software malicioso que pode prejudicar um computador ou roubar informações. Inclui vírus, spyware e ransomware.
- **Microsoft Teams** – Plataforma digital usada para comunicação e colaboração online, especialmente em ambiente escolar e profissional.

N

- **Navegador (Browser)** – Programa que permite navegar na Internet, como o Google Chrome, Mozilla Firefox ou Microsoft Edge.

O

- **Open-source (Código aberto)** – Software cujo código está disponível para que qualquer pessoa possa usar, modificar ou melhorar.
- **Operadores de pesquisa** – Comandos que ajudam a melhorar pesquisas na Internet (exemplo: **site:** para pesquisar dentro de um site específico).

P

- **Photopea** – Editor de imagens online gratuito, semelhante ao Photoshop.

- **Phishing** – Técnica usada por hackers para enganar pessoas e obter informações confidenciais, como senhas e dados bancários.
- **Privacidade online** – Proteção dos dados e informações pessoais na Internet.

R

- **Ransomware** – Tipo de malware que bloqueia ficheiros ou sistemas e exige um pagamento para desbloqueá-los.
- **Redes sociais** – Plataformas digitais onde os utilizadores partilham conteúdos e interagem (exemplo: Instagram, TikTok, Facebook).

S

- **Screenshot (Captura de ecrã)** – Imagem tirada do ecrã do computador ou telemóvel.
- **Segurança digital** – Práticas para proteger informações pessoais e dispositivos eletrónicos.
- **Senhas seguras** – Palavras-passe fortes que incluem letras, números e símbolos para dificultar o acesso por hackers.
- **Sistema operativo** – Software principal de um computador, como **Windows** ou **Linux**, que gere todos os programas e funções.

T

- **TinEye** – Site que permite fazer pesquisa por imagem para verificar a sua origem.
- **Trojan (Cavalo de Troia)** – Tipo de malware disfarçado de programa legítimo que pode roubar dados ou controlar um computador.

V

- **Vírus informático** – Programa malicioso que se espalha entre dispositivos e pode danificar ficheiros ou roubar informações.

W

- **Windows** – Sistema operativo pago, desenvolvido pela Microsoft, utilizado na maioria dos computadores pessoais.
- **Wi-Fi público** – Redes de Internet abertas que podem ser perigosas porque não são seguras.
- Agora já tens uma **lista rápida de consulta** para todos os termos que encontraste no livro!

QUESTÕES DE REFLEXÃO

Estas questões vão ajudar-te a refletir sobre os temas do eBook.

Microsoft Teams

1. Para que serve o Microsoft Teams e como pode ser útil na escola?
2. Que funcionalidades do Microsoft Teams permitem a colaboração entre alunos e professores?
3. Como podes partilhar um ficheiro com os teus colegas no Teams?
4. Qual é a importância das reuniões virtuais na educação?
5. O que acontece se fores adicionado a uma equipa no Microsoft Teams?
6. Como podes organizar as tuas tarefas dentro do Teams?
7. Porque é importante utilizar o chat de forma responsável?
8. Como podes aceder a uma aula gravada no Teams?
9. Qual a diferença entre um canal público e um canal privado dentro do Teams?
10. O Microsoft Teams pode ser utilizado apenas no computador?

Segurança na Internet – Proteção da Identidade e Senhas

11. O que faz com que uma palavra-passe seja segura?
12. Porque não deves usar a mesma senha em vários sites?
13. O que é a Autenticação em Dois Fatores (2FA) e como pode proteger-te?
14. Como podes criar uma senha difícil de adivinhar, mas fácil de lembrar?
15. O que é o phishing e como podes evitar cair nessa armadilha?
16. O que nunca deves partilhar online para proteger a tua identidade digital?
17. Como podes saber se um site é seguro para introduzires os teus dados pessoais?
18. Qual é a diferença entre uma senha forte e uma senha fraca?
19. O que deves fazer se desconfiares que a tua conta foi comprometida?
20. Como podes configurar a segurança da tua conta de email ou rede social?

Mensagens Falsas e Manipuladas (Fake News)

21. Como podes distinguir uma notícia falsa de uma verdadeira?
22. O que são fact-checkers e como te podem ajudar?

Publicado em março de 2025.

23. Como podes confirmar se uma imagem que viste na Internet é verdadeira?
24. Porque é que algumas fake news se espalham tão rapidamente?
25. O que deves fazer antes de partilhares uma notícia com os teus amigos?
26. Como podes verificar a credibilidade de um site de notícias?
27. As fake news existem apenas nas redes sociais? Explica.
28. Como podes ensinar outras pessoas a não caírem em notícias falsas?
29. O que significa "pensar criticamente" quando lês algo na Internet?
30. Como podes usar a pesquisa por imagem reversa para verificar a veracidade de uma foto?

Sistemas Operativos – Windows e Linux

31. O que é um sistema operativo e qual é a sua função?
32. Quais são as principais diferenças entre o Windows e o Linux?
33. Porque é que o Linux é considerado um sistema de código aberto?
34. Em que situações pode ser vantajoso usar o Windows?
35. Em que situações pode ser vantajoso usar o Linux?
36. O que significa dizer que um sistema operativo é proprietário?
37. Quais são alguns exemplos de sistemas operativos além do Windows e Linux?
38. O Windows e o Linux podem ser instalados no mesmo computador? Explica.
39. Como podes instalar um novo sistema operativo no teu computador?
40. O que deves considerar antes de escolher um sistema operativo?

Utilização de Antivírus e Proteção contra Malware

41. Para que serve um antivírus e como ele te protege?
42. Qual é a diferença entre vírus, malware, spyware e ransomware?
43. Como podes evitar que o teu computador fique infetado com malware?
44. Porque não deves descarregar ficheiros de sites desconhecidos?
45. O que deves fazer se o teu antivírus detetar uma ameaça?
46. Como podes verificar se um email suspeito contém malware?
47. Como funcionam os ataques de ransomware e como podes proteger-te?
48. O que é uma firewall e como ela melhora a segurança digital?
49. Como podes manter o teu computador atualizado para evitar ataques?
50. Porque deves ter cuidado ao clicar em links enviados por desconhecidos?

Publicado em março de 2025.

Pesquisa na Internet e Navegadores Web

51. O que é um navegador web e qual é a sua função?
52. Qual é a diferença entre um navegador e um motor de busca?
53. Como podes melhorar a tua pesquisa no Google usando operadores de pesquisa?
54. Como podes verificar se um site é confiável?
55. Porque não deves confiar cegamente na primeira página de resultados do Google?
56. O que significa "HTTPS" na barra de endereços de um site?
57. Como podes encontrar imagens livres de direitos de autor na Internet?
58. Porque é importante verificar a data de publicação de uma informação?
59. Como podes usar o Google Lens para pesquisar uma imagem?
60. O que significa "navegação anónima" e quando pode ser útil?

Edição de Imagem – GIMP e Photopea

61. O que é uma imagem bitmap e como se diferencia de uma imagem vetorial?
62. Quais são as principais ferramentas do GIMP e do Photopea para editar imagens?
63. Como podes remover o fundo de uma imagem no Photopea?
64. Porque deves ter cuidado ao manipular imagens na Internet?
65. O que significa "direitos de autor" no uso de imagens digitais?
66. Quais são as vantagens do GIMP em relação a editores pagos?
67. Como podes adicionar texto a uma imagem no Photopea?
68. Qual é a diferença entre os formatos PNG e JPG?
69. O que significa trabalhar com camadas numa edição de imagem?
70. Como podes criar um cartaz digital usando ferramentas gratuitas?

Funções do Teclado e Atalhos Úteis

71. O que são atalhos de teclado e porque são úteis?
72. Qual é a função das teclas Ctrl, Shift e Alt?
73. Como podes alternar entre janelas abertas no Windows usando o teclado?
74. Qual é o atalho para copiar e colar um texto?
75. Como podes escrever o símbolo **@** num teclado português?
76. Qual é o atalho para tirar um screenshot no Windows?
77. Como podes mudar rapidamente de idioma no teclado?

78. Qual a importância de conhecer atalhos de teclado na escola e no trabalho?
79. Como podes aceder rapidamente ao explorador de ficheiros usando atalhos?
80. Como podes formatar um texto rapidamente no Word usando o teclado?

Segurança na Internet – Proteção de Senhas e Identidade Digital

81. Porque deves evitar publicar informações pessoais nas redes sociais?
82. O que deves fazer se receberes uma mensagem suspeita a pedir os teus dados?
83. Como podes configurar a privacidade da tua conta numa rede social?
84. O que significa engenharia social em segurança digital?
85. Como podes proteger a tua identidade digital no dia a dia?
86. Quais são as consequências de partilhar demasiada informação pessoal online?
87. Porque deves evitar aceitar pedidos de amizade de desconhecidos?
88. O que deves fazer se descobrires que alguém criou um perfil falso com os teus dados?
89. Como podes denunciar conteúdos inapropriados nas redes sociais?
90. Porque é importante ter um comportamento responsável no mundo digital?

Estas perguntas vão ajudar-te a **pensar criticamente** sobre cada tema e a preparar-te melhor para o teste.