Study Guide Transcript

Spring 2025

This study guide transcript has been provided to support learners in following the ***Workplace Digital Skills*** *course.*

While the guide serves as a useful resource, we highly recommend that learners watch the course episodes on the ***Way2Learn channel*** *or via the* ***Video-on-Demand*** *service to gain a full understanding before completing the answer book.*

For your convenience, episode times are listed on ***page 4 of the answer book****, within the* ***Way2Learn prospectus*** *in your library, and in the* ***quick-glance guide****.*

Episode 1: Using and Managing Information

Introduction

The digital age has transformed how we work, shop, socialise, and learn. With 90% of jobs requiring some level of digital competency, mastering digital skills is no longer optional—it is essential. Employers seek individuals who can efficiently locate, manage, and protect digital information.

This episode explores how search engines work, advanced search techniques, and best practices for storing and managing information securely.

How Search Engines Work

Search engines act as vast digital libraries, scanning millions of webpages to provide relevant results. But how do they decide what to show? They use three key processes:

1. **Crawling** – Automated programs, known as bots or spiders, scan the internet, discovering and collecting new or updated content.
2. **Indexing** – The discovered content is categorised and stored in a database, ready to be retrieved when needed.
3. **Ranking** – When a user enters a search query, the search engine sorts the indexed content and displays the most relevant results based on factors such as keywords, page popularity, and reliability.

Understanding these processes allows users to refine their search techniques, ensuring they find the most relevant and trustworthy information.

Refining Your Search: Advanced Techniques

Not all searches produce useful results. If a search returns millions of webpages, filtering the results becomes essential. Here are some effective strategies:

- **Boolean Operators** – Using words such as AND, OR, and NOT helps narrow or expand searches.
  - Example: Searching "workplace safety AND regulations" will only return results containing both terms.
- **Phrase Searching** – Quotation marks (" ") can be used to find an exact phrase.
  - Example: Searching **"data protection policies"** will only return pages with that exact phrase.
- **Filtering by Date** – Ensures information is recent and relevant. Many search engines allow filtering results to show only pages from the past year.
- **Domain-Specific Searches** – Searching within trusted domains such as **.gov** or **.edu** increases the likelihood of finding credible sources.
  - Example: Searching "cybersecurity site:.gov" will return only government sites with cybersecurity information.
- **Subject Searching** – If keyword searches return too many irrelevant results, using subject categories can refine searches further.

Evaluating Information: Is It Reliable?

Not all online sources are trustworthy. Anyone can publish content, so it is important to evaluate credibility. A common method is the CRAAP test, which assesses:

- **C**urrency – Is the information recent and up to date?
- **R**elevance – Does the content directly relate to what you need?
- **A**uthority – Is the source reputable (e.g., government, academic, or industry-recognised websites)?
- **A**ccuracy – Are facts supported by evidence and reliable references?
- **P**urpose – Is the content objective, or does it show bias?

Before using information, particularly in a professional setting, always verify its accuracy by cross-referencing multiple sources.

Storing and Managing Digital Information

Once useful information is found, it must be stored securely and efficiently. Poor organisation can lead to lost data, wasted time, and security risks.

Best practices for managing digital files:

- **Use Clear Folder Structures** – Organising files by topic, date, or project makes retrieval easier.
- **Follow Naming Conventions** – Descriptive file names (e.g., "Employee_Safety_Report_2025.pdf") improve searchability.
- **Use Bookmarks for Quick Access** – Web browsers allow users to save important pages for future reference. In Chrome, bookmarks can be accessed via the three-dot menu, while Internet Explorer uses the "Favourites" feature.
- **Regular Housekeeping** – Deleting outdated files and using cloud storage or external drives prevents data loss.
- **Data Security** – Sensitive information should be stored in **password-protected** files or **encrypted** storage systems.

Following these strategies ensures that digital information remains accessible and secure.

Scenario: Applying Your Digital Skills at Work

Imagine you are researching recent **cybersecurity threats** for a workplace report. You find multiple sources, but some provide contradictory information. How would you determine which is most reliable?

1. **Check the Source** – Government and educational sites (**.gov**, **.edu**) are more credible than unknown blogs.
2. **Verify the Date** – Recent publications are more likely to contain accurate, up-to-date data.
3. **Cross-Reference** – Comparing findings from multiple reputable sources helps confirm accuracy.

Using these steps ensures that your report is based on trustworthy information.

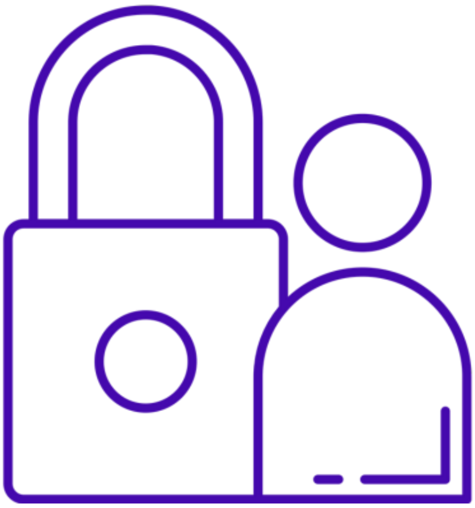
Summary

- Search engines use crawling, indexing, and ranking to organise information.
- Advanced search techniques such as Boolean operators, filters, and domain-specific searches help refine results.
- Evaluating credibility using the CRAAP test ensures information is reliable.
- Organising and storing information effectively improves accessibility and security.

By mastering these skills, you will be able to find, assess, and manage digital information confidently—an essential competency in today's workplace.

Now, work through the Answer Book tasks for this episode before moving on to Episode 2.

Episode 2: Trusting and Organising Information



The Challenge of Digital Information

The internet provides instant access to an overwhelming amount of information. With over 1 billion websites, anyone can publish content—from news articles and academic papers to blogs and social media posts. While this makes knowledge more accessible than ever, it also creates a problem: how do we know which sources are trustworthy?

In this episode, we will explore how to evaluate the credibility of online information using the CRAAP test and discuss best practices for organising digital files effectively.

Evaluating the Reliability of Information

Not all online information is accurate, unbiased, or up to date. To determine whether a source can be trusted, we use the CRAAP test:

Currency

- Is the information recent?
- Is the content still relevant?
- Example: A 2010 article on cybersecurity is likely outdated due to rapid technological advancements.

Relevance

- Does the information directly answer your question?
- Is it written at the right level of detail for your needs?
- Example: A blog post about workplace safety may be interesting but not as useful as official health & safety guidelines.

Authority

- Who is the author or organisation behind the information?
- Are they qualified in this subject?
- Example: You would trust financial advice from a bank's website more than from a random Twitter post.

Accuracy

- Is the content supported by evidence, references, or expert review?
- Can the facts be verified on other reliable sources?
- Example: Wikipedia is a good starting point but should not be used as a final source because anyone can edit it.

Purpose

- Is the content informative, persuasive, or biased?
- Does it try to sell you something or influence your opinion?
- Example: A website that reviews cameras but has an advertising partnership with one brand may be biased.

By applying the CRAAP test, we can think critically about the information we find and make informed decisions.

The Importance of File Organisation

Just like physical documents, digital files need to be well-organised. Poor organisation leads to wasted time, lost information, and confusion.

Imagine searching for a workplace policy document and finding files labelled "New.doc" or "Final_Version_2". Without a structured system, locating important information becomes frustrating and inefficient.

Best Practices for Digital File Organisation:

✓ **Use Clear Folder Names** – Folders should be named logically, based on content.

✓ **Follow a Consistent Structure** – If using dates, always follow the same format (e.g., **2025-03-15** instead of **March 15 2025**).

✓ **Avoid Over-Nesting** – Too many subfolders make files harder to find.

✓ **Use Descriptive File Names** – Instead of "Document1.docx", use "Health_and_Safety_Report_2025.docx".

✓ **Store Files in the Right Location** – Keep work-related files in designated folders, not mixed with personal documents.

Scenario: Applying These Skills in the Workplace

You are working for a company that stores all employee records in a single folder, with files named inconsistently. This leads to confusion and accidental deletion of important documents.

To improve the system:
Introduce structured subfolders (e.g., organise by department or year).

Use clear naming conventions (e.g., "Employee_John_Doe_Contract_2025.pdf").
Restrict access to sensitive files to prevent accidental edits or deletions.

A well-structured file system improves efficiency, reduces errors, and ensures compliance with company procedures.

Summary

- The internet contains both reliable and unreliable information—learning to evaluate sources is essential.
- The CRAAP test (Currency, Relevance, Authority, Accuracy, Purpose) helps assess credibility.
- Poorly organised digital files cause confusion and inefficiency.
- Using structured folder systems and clear file names improves digital organisation.

Now, complete the Answer Book tasks for this episode before moving on to Episode 3.

Episode 3: Keeping Safe Online

Introduction

The internet is essential for modern work and communication, but it also comes with risks. Personal data, financial details, and company information are valuable targets for cybercriminals. Understanding how to protect yourself and your organisation from cyber threats is a vital digital skill.

Understanding Personal Data and Digital Footprints

Personal data is any information that can be used to identify a living person. This includes:

✓ Name, address, and email
✓ Bank details and identification numbers
✓ Location history and online activity

Whenever you browse the internet, use social media, or shop online, you leave behind a digital footprint. This includes:

- Websites you visit
- Searches you make
- Details entered into online forms

Cybercriminals collect and use this data to commit fraud, steal identities, or even hold sensitive information for ransom. Understanding what personal data is and how it can be misused is the first step in staying safe online.

Common Cyber Threats

Cyberattacks come in many forms. Some of the most common include:

Phishing Attacks

Phishing is when a hacker tricks you into giving away sensitive information. This is often done through emails pretending to be from a bank, employer, or trusted organisation.

Signs of a phishing email:
❌ **Urgent language** – "Your account will be locked unless you respond immediately!"
❌ **Suspicious links** – Hover over links before clicking to check the real URL.
❌ **Unknown sender** – If the sender's email address looks slightly off (e.g., "yourbank@security-alert.com"), it may be fake.

➞ How to stay safe: Never click on links in suspicious emails. If in doubt, contact the organisation directly using official contact details.

Malware and Viruses

Malware (short for malicious software) is designed to damage or steal information. Common types include:
✓ **Viruses** – Infect files and spread across devices.
✓ **Trojans** – Disguised as legitimate software but secretly cause harm.
✓ **Ransomware** – Locks files and demands payment for access.

➞ **How to stay safe:**

- Install and update antivirus software.
- Avoid downloading files from unknown sources.
- Don't open email attachments unless you trust the sender.

Public Wi-Fi Attacks

Free Wi-Fi networks in cafes, airports, and hotels can be risky. Hackers can intercept your data if the network is not secure.

➞ How to stay safe:
✓ Avoid logging into banking sites or sensitive accounts on public Wi-Fi.
✓ Use a VPN (Virtual Private Network) to encrypt your internet connection.

Protecting Organisational Data

Businesses must follow strict security protocols to protect employee and customer data. This includes:

✓ Strong Password Policies – Employees should use unique, complex passwords and enable two-factor authentication (2FA) where possible.
✓ Data Encryption – Sensitive files should be encrypted to prevent unauthorised access.
✓ Access Controls – Employees should only have access to the data they need for their job.
✓ Cybersecurity Training – Staff must be educated on recognising and reporting security threats.

➞ Reporting a Security Breach:
If you suspect a data breach, report it immediately to your employer's IT department. Under GDPR (General Data Protection Regulation), organisations must report major breaches within 72 hours to the Information Commissioner's Office (ICO).

Recognising Insecure Websites

Hackers sometimes create fake websites that look like real ones to steal login credentials. Before entering personal details, check for:

✓ HTTPS in the address bar – Secure websites use https:// instead of http://.
✓ Spelling errors in the URL – Fraudulent sites often have small spelling differences (e.g., amaz0n.com instead of amazon.com).
✓ Unusual pop-ups – Be wary of sudden requests for passwords or payments.

Scenario: Avoiding a Cybersecurity Mistake at Work

You receive an email claiming to be from your company's HR department, asking you to click a link to confirm your personal details.

How should you respond?
C**heck the sender's email address** – Does it match your company's official domain?
Look for spelling and grammar mistakes – Poorly written emails are a red flag.
Do not click the link – Instead, contact HR directly using official channels.

By taking these steps, you protect both yourself and your organisation from potential cyber threats.

Summary

- Personal data can be exploited by cybercriminals if not protected properly.
- Phishing attacks, malware, and public Wi-Fi risks are common online threats.
- Businesses must follow strict data security policies to protect sensitive information.
- Verifying website security and avoiding suspicious emails can help prevent cyberattacks.

Now, complete the Answer Book tasks for this episode before moving on to Episode 4.

Episode 4: The Law and Your Data

Introduction

In today’s digital world, businesses collect thousands of pieces of personal data every week. This information includes names, addresses, browsing habits, and even medical records. Often, individuals are unaware of how much data is being gathered about them because they do not read the fine print when signing up for services.

Data is valuable, and if misused, it can pose risks to individuals and organisations. This is why privacy and data protection laws exist—to ensure that personal data is handled securely and fairly.

Privacy vs. Data Protection

Although often used interchangeably, privacy and data protection are not the same.

✓ Privacy refers to a person’s right to control their own personal information. It is a fundamental human right, recognised in Article 12 of The Universal Declaration of Human Rights.

✓ Data Protection focuses on how businesses and organisations collect, store, and use personal data. It ensures that information is handled responsibly and securely.

➞ Example: You have the right to privacy over your medical records, and hospitals must follow data protection laws to ensure those records are kept secure.

The General Data Protection Regulation (GDPR) and Data Protection Act (DPA)

To protect people's personal data, strict laws are in place.

✓ GDPR (General Data Protection Regulation) is an EU law that gives individuals more control over how their data is collected and used.

✓ The UK Data Protection Act (DPA 2018) was introduced alongside GDPR to enforce these regulations in the UK.

Key Principles of GDPR & DPA:

Fair and Transparent Processing – Businesses must inform individuals about what data they collect and why.
Limited Use – Data can only be collected and used for specific purposes.
Minimisation – Only necessary data should be collected.
Accuracy – Data must be kept up to date.
Storage Limits – Data should not be kept longer than needed.
Security Measures – Organisations must protect data against breaches.

➞ Failure to comply with GDPR and DPA can result in significant fines.

How Businesses Protect Data

Organisations must take steps to keep personal data secure. Some of these include:

✓ Restricting Access – Only authorised employees should have access to sensitive information.

✓ Using Strong Passwords and Encryption – This prevents unauthorised access to data.

✓ Cybersecurity Policies – Employees should be trained on how to recognise cyber threats.

✓ Data Classification – Important data should be labelled as confidential to ensure it is handled correctly.

➞ Businesses that fail to protect personal data risk financial penalties and reputational damage.

What Happens When a Data Breach Occurs?

A data breach happens when personal data is lost, stolen, or accessed by unauthorised individuals. This can occur due to:

- Cyberattacks (e.g., hacking, phishing scams).
- Human error (e.g., sending sensitive information to the wrong person).
- Poor security practices (e.g., weak passwords or unencrypted files).

Under GDPR, businesses must:
✓ Report serious breaches to the Information Commissioner's Office (ICO) within 72 hours.
✓ Inform affected individuals if their personal data has been exposed.
✓ Keep a record of all breaches, even minor ones.

➞ Data breaches can lead to legal action, fines, and loss of customer trust.

Scenario: A Costly Mistake

A company's HR department stores employee records in a shared folder without setting proper privacy restrictions. A junior employee accidentally shares a document containing staff salaries with the entire workforce.

➞ What went wrong?
❌ No access controls were in place—confidential information should only be available to relevant staff.
❌ The company failed to follow data protection policies, putting employees' privacy at risk.

➞ What should have been done?
- Restrict access – Only HR personnel should have permission to view salary records.
- Train staff – Employees must understand the importance of data security.

By following GDPR and DPA guidelines, organisations can prevent costly mistakes like this one.

Protecting Data as an Employee

✓ **Check Privacy Settings** – Ensure documents shared online are only visible to the correct people.

✓ **Think Before Sharing** – Ask yourself: *Could this information be misused?*

✓ Use Secure Storage – Keep sensitive files in password-protected or encrypted folders.

✓ Follow Company Policies – Every organisation has data protection procedures that employees must follow.

➞ If you suspect a data breach, report it immediately.

Summary

- Privacy and data protection ensure personal information is handled responsibly.
- GDPR and DPA protect individuals and require businesses to keep data secure.
- Failing to protect data can lead to financial penalties, legal action, and reputational damage.
- Employees must follow best practices to keep business and personal data safe.

Now, complete the Answer Book tasks for this episode before moving on to Episode 5.

Episode 5: Communicating Online

Introduction

Technology has changed the way we interact with others. Emails, social media, and messaging platforms allow us to connect instantly, whether socially or professionally. However, with constant connectivity comes responsibility.

Choosing the Right Communication Method

Different platforms are used for different purposes.

Social vs. Professional Communication:

✓ Social Media (e.g., Facebook, Instagram, Twitter) – Used for personal interactions but can impact your professional reputation.
✓ Professional Networks (e.g., LinkedIn, company intranets) – Best for career-building, networking, and work-related discussions.
✓ Email – Used in business settings for formal communication.
✓ Instant Messaging (e.g., WhatsApp, Microsoft Teams, Slack) – Useful for quick workplace conversations but should not replace formal emails.

➞ Think before you post or send a message—your online communication can have lasting consequences.

The Dangers of Oversharing Online

Many people share personal details online without realising the risks.

Example: A Risky Social Media Post

"Hi everyone! Off on holiday this weekend. Can't wait to spend loads of money and relax!"

What does this post reveal?
-Your house will be empty – Criminals could see this as an opportunity for burglary.

- Financial risk – A bank reviewing your credit application may see your spending habits as a concern.
- Professional impact – A potential employer might question your attitude towards money or work responsibilities.

➞ Solution: Adjust your privacy settings and think before posting!

Once something is online, it can be shared, copied, and stay visible forever. Always ask yourself:
✓ Would I want my employer or family to see this?
✓ Could this post affect my reputation or security?

Understanding Cookies and Online Privacy

Many websites track users through cookies, which store information about browsing habits, login details, and shopping preferences. While they can improve user experience by remembering settings, they also allow companies to collect significant amounts of personal data.

To maintain privacy:

- Clear cookies regularly through browser settings.
- Decline unnecessary cookies when prompted.
- Use private browsing modes where possible.

These steps help reduce digital footprints and limit how much information companies can gather.

Using Email Professionally

Email is a key communication tool in the workplace, but it must be used carefully to maintain professionalism. A poorly written or misinterpreted email can lead to confusion, conflict, or even disciplinary action.

Best Practices for Professional Emails

1. **Use a clear subject line** – This helps recipients understand the purpose of the email immediately.
2. **Keep the message structured and concise** – Avoid unnecessary detail and get to the point quickly.
3. **Maintain a professional tone** – Avoid slang, abbreviations, or overly casual language.
4. **Proofread before sending** – Spelling and grammar mistakes can appear unprofessional.
5. **Use CC and BCC appropriately** – Copy in only necessary recipients and use BCC when protecting privacy.

A professional email should always be polite and well-structured. Instead of writing *"Hey, can you send that report?"*, a better approach would be:

Subject: Request for Report Submission

Dear [Recipient’s Name],

I hope you are well. Please could you send me the latest version of the report at your earliest convenience? Let me know if you need any further details.

Best regards,
[Your Name]

This email is clear, polite, and professional.

Recognising Phishing Emails

Phishing scams are a major online threat. These emails attempt to trick recipients into clicking harmful links or sharing confidential information by pretending to be from a trusted source.

Signs of a phishing email include:

- Urgent language pressuring immediate action, such as *"Your account will be closed unless you respond now."*
- Suspicious links that do not match the official website address.
- Unexpected attachments that could contain malware.

To stay safe, check the sender's details carefully and hover over links before clicking them. If an email seems suspicious, contact the organisation directly through official channels rather than replying or clicking any links.

Managing Workplace Emails

A cluttered inbox can lead to missed deadlines and lost information. Managing emails efficiently improves productivity and reduces stress.

To stay organised:

- Set up email folders for different projects or departments.
- Schedule times to check emails rather than responding instantly to every message.
- Use out-of-office replies when unavailable for an extended period.

A well-managed inbox ensures that important messages are not overlooked.

Using Social Media for Business

Social media is not just for personal use—it can also be a powerful tool for businesses. Companies use platforms like Facebook, Twitter, and LinkedIn to promote services, engage with customers, and build brand recognition.

One example is a bakery that ran a Facebook competition asking customers to share why their mother deserved a special treat for Mother's Day. By doing so, the bakery increased engagement and boosted sales.

For businesses, social media provides an opportunity to interact directly with customers and attract new ones. However, it is important to manage company accounts professionally and avoid controversial topics that could damage the brand's reputation.

Summary

- Different communication tools serve different purposes—email remains the most common professional method.
- Oversharing personal information online can have unintended consequences.
- Understanding cookies and privacy settings can help protect digital information.
- Professional email etiquette is essential for clear and respectful workplace communication.
- Social media can be a valuable business tool when used effectively.

Now, complete the **Answer Book tasks** for this episode before moving on to Episode 6.

Episode 5: Digital Career Development

Introduction

In today's world, social media and online presence play a significant role in employment prospects. Employers frequently search candidates' online profiles before making hiring decisions. A single post, photo, or comment could affect job opportunities, while a well-managed digital identity can help advance your career.

This episode explores how to:

- Manage and promote a professional digital identity.
- Use the internet and social media for job searching.
- Leverage technology for career development and continuous learning.

Understanding these areas will help you take control of your online presence and create opportunities for professional success.

The Impact of Social Media on Employment

Employers often review job candidates' online presence as part of the hiring process. Even posts made years ago can be found and used to assess your character, judgment, and professionalism.

Example: A Costly Social Media Post

A candidate posts on Facebook about stealing items from a pub after a night out. The post is meant as a joke among friends, but a potential employer sees it. Even if the post was not serious, it could make the employer question the candidate's integrity, leading them to reject the application.

To avoid harming employment prospects:

- **Keep personal and professional accounts separate**—use different platforms for work and social life.
- **Check privacy settings**—ensure only trusted individuals can see personal posts.
- **Avoid controversial topics**—negative or offensive content can reflect poorly on your character.

A strong professional online identity enhances your employability, while careless social media use can have lasting consequences.

Building a Professional Online Presence

Your online identity should showcase your skills, experience, and professionalism. Employers may search for your name online, so it's important that the results represent you well.

Steps to Improve Your Digital Reputation:

1. **Search your own name** – See what appears and remove or adjust any negative content.
2. **Optimise professional profiles** – Ensure LinkedIn and other career platforms reflect your skills and achievements.
3. **Create industry-relevant content** – Sharing articles, insights, or work projects demonstrates knowledge and engagement.
4. **Use a professional profile picture** – Avoid casual or inappropriate images on professional accounts.

A well-managed digital identity helps employers see you as a credible and competent professional.

Using the Internet and Social Media for Job Searching

Many job opportunities are advertised online, but finding the right roles requires strategy.

Where to Look for Jobs Online:

- **Company websites** – Many organisations post vacancies directly on their websites.
- **Job search engines** – Sites such as Indeed, Reed, LinkedIn Jobs, and Glassdoor list thousands of opportunities.
- **Social media** – Following industry leaders and joining professional groups can lead to job referrals.
- **Networking platforms** – LinkedIn is a key tool for connecting with employers and recruiters.

When applying for jobs, tailor CVs and cover letters to each position. Highlight relevant skills and **use keywords from job descriptions** to improve visibility.

Researching Employers Before an Interview

Understanding a company before an interview can provide a competitive advantage. Researching helps tailor answers to interview questions and demonstrates genuine interest in the role.

How to Research a Company Effectively:

- **Visit the company website** – Learn about its mission, values, and latest news.
- **Check news articles** – Look for recent achievements, challenges, or developments.
- **Read employee reviews** – Sites like Glassdoor provide insight into workplace culture.
- **Explore social media presence** – Company LinkedIn pages and Twitter accounts often highlight key priorities.

By gathering this information, you can confidently answer questions such as “Why do you want to work for us?” and stand out from other candidates.

Using Technology for Career Progression

Career development doesn’t stop after securing a job. The digital world offers continuous learning opportunities to help professionals grow and stay competitive.

Ways to Use Technology for Career Growth:

- Online courses – Platforms like Coursera, LinkedIn Learning, and Udemy offer training in key skills.
- Webinars and virtual conferences – Industry events provide networking and professional development opportunities.
- Professional forums and blogs – Engaging in online discussions can build expertise and credibility.
- Personal branding – Maintaining a blog or portfolio website can showcase skills and attract new opportunities.

By actively using these tools, professionals can stay ahead in their careers and adapt to industry changes.

Summary

- Employers assess online profiles when considering candidates, making **digital** reputation management essential.
- A strong professional presence on platforms like LinkedIn improves employability, while careless social media use can harm career prospects.
- Job seekers should use the internet strategically to find opportunities and research companies before interviews.
- Continuous learning through online courses, networking, and industry engagement supports long-term career success.

Now, complete the Answer Book tasks for this episode.