4565: Computing Foundations for a Digital Age
Unit 2

# Jeopardy Questions

Use this link to create a Jeopardy game board: https://jeopardylabs.com/

## 1️⃣ Digital Footprint

- *Understanding how online actions leave a trail.*

**100: What is a digital footprint?**
The record of everything you do online, including posts, comments, and searches.

**200: Name one place where someone can find your digital footprint.**
Social media, search engines, websites, online shopping history.

**300: True or False: Deleting a post completely erases it from the internet.**
False. Even deleted posts may be archived, screenshotted, or stored on backup servers.

**400: What are two ways to manage your digital footprint?**
Adjust privacy settings, think before posting, delete unused accounts, use strong passwords.

**500: How can a digital footprint affect future opportunities (college, jobs, etc.)?**
Employers and colleges review online activity, and inappropriate content may impact decisions.

---

## 2️⃣ Online Privacy vs. Security

- *Knowing the difference between protecting information & staying secure.*

**100: What is the main difference between privacy and security?**
Privacy protects personal information; security defends against cyber threats.

**200: Give an example of a privacy setting you can adjust on social media.**
Make accounts private, limit who sees posts, disable location tracking.

**300: True or False: A strong password is enough to completely secure an account.**
False. Two-factor authentication and other measures are needed.

**400: What is an example of a situation where privacy and security conflict?**
Encryption protects privacy but can make it harder for security agencies to track criminals.

**500: Explain why companies track user data and how that affects privacy.**
Companies collect data for advertising, but it can be misused or sold.

---

## 3️⃣ Password Protection

- *How to create and manage strong passwords.*

**100: What is one thing you should never include in your password?**
Your name, birthday, personal info, or the word "password"

**200: What is two-factor authentication (2FA)?**
A security feature that requires a second form of verification (e.g., code sent to phone).

**300: True or False: You should use the same password for multiple accounts.**
False. Each account should have a unique password.

**400: Name three characteristics of a strong password.**
Long, complex (mix of letters, numbers, symbols), and not easily guessed.

**500: You get an email asking you to 'reset your password immediately' with a suspicious link. What should you do?**
Don't click the link. Visit the official site directly or report the email.

---

## 4️⃣ Cyber Threats & Scams

- *Recognizing and avoiding online dangers.*

**100: What is phishing?**
A scam where hackers trick users into giving personal info via fake emails or websites.

**200: What is the purpose of a firewall?**
To block unauthorized access to a computer or network.

**300: Name two common types of malware.**
Viruses, ransomware, spyware, trojans, worms.

**400: What should you do if you receive an email saying you won a contest you never entered?**
Don't click links, report it as spam, and delete the email.

**500: How does social engineering trick people into giving away personal information?**
By manipulating trust (e.g., pretending to be a friend, coworker, or authority figure).

---

## 5️⃣ Social Media Safety

- *Protecting personal information online.*

**100: Why should you avoid sharing personal details (like your full name) publicly?**
To prevent identity theft and stalking.

**200: What is an example of oversharing online?**
Posting vacation plans, home address, or school name.

**300: True or False: It's safe to accept friend requests from strangers on social media.**
False. They could be scammers or impersonators.

**400: What are two risks of geotagging your posts?**
Revealing your location to strangers, making you a target for theft.

**500: How can adjusting privacy settings help protect your social media accounts?**
Limits who can see posts, preventing data collection and cyberstalking.

---

## 6️⃣ Cybersecurity Best Practices

- *Everyday actions to stay safe online.*

**100: Why is it important to update your software regularly?**
To patch security vulnerabilities.

**200: What is a VPN, and how does it help with security?**
A Virtual Private Network encrypts internet traffic, protecting data from hackers.

**300: Name two ways to recognize a scam website.**
Poor design, missing HTTPS, too-good-to-be-true offers, spelling errors.

**400: Why should you be careful when using public Wi-Fi?**
Hackers can intercept data on unsecured networks.

**500: Explain why companies use encryption to protect data.**
Encryption scrambles data so only authorized parties can read it.

---

## 7️⃣ Data Breaches & Hacking

- *What happens when security fails.*

**100: What is a data breach?**
Unauthorized access to private data.

**200: Name one major company that has experienced a data breach.**
Equifax, Facebook, Target, Yahoo, etc.

**300: What should you do if your password is exposed in a data breach?**
Change it immediately and enable two-factor authentication.

**400: What is ethical hacking, and how is it different from criminal hacking?**
Ethical hackers test security legally to help fix vulnerabilities.

**500: How do hackers use ransomware to attack people or businesses?**
They lock files and demand payment for access.

---

## 8️⃣ Emerging Technologies & Cyber Risks

- *How AI, deepfakes, and more impact security.*

**100: What is artificial intelligence (AI)?**
Technology that mimics human thinking.

**200: How do deepfakes pose a cybersecurity threat?**
They create fake videos that can spread misinformation.

**300: What is biometric authentication (e.g., fingerprint or face recognition)?**
Security that verifies identity using unique physical traits.

**400: How could self-driving cars be hacked?**
Hackers could take control or disable safety features.

**500: Why is cybersecurity becoming more important as technology advances?**
More devices are connected, increasing risks of cyberattacks.

---

## 9️⃣ Safe Internet Browsing

- *How to avoid dangers while online.*

**100: What is a secure website's URL supposed to start with?**
HTTPS (not HTTP).

**200: Why should you avoid clicking on pop-up ads?**
They may contain malware or scams.

**300: What is a cookie in terms of internet browsing?**
A small file that stores website data about you.

**400: How can private browsing (incognito mode) help protect privacy?**
It prevents storing history and cookies.

**500: What are browser extensions, and how can they improve security?**
Small add-ons that block ads, track cookies, or enhance security.

---

## 🔟 Cyber Laws & Ethics

🔹 *Legal and ethical responsibilities online.*

**100: What is cyberbullying?**
Harassing or threatening others online.

**200: Is it legal to download movies or music for free from an unknown website? Why or why not?**
No, it's piracy and violates copyright laws.

**300: What is the purpose of copyright laws online?**
To protect creators' work from being used without permission.

**400: Why is it important to get permission before sharing someone else's photo online?**
It respects privacy and avoids legal issues.

**500: What is the Computer Fraud and Abuse Act (CFAA)?**
A U.S. law against unauthorized access to computers.