

Protecting Workplace Data and Responding to Cybersecurity Risks

Detailed practice, calculation, decision-making, and assessment

GRADES 9-12	TIME 2 x 42 min	GROUPING I / pairs / whole	PRODUCT Protocol
YOUR CHALLENGE Classify information, detect phishing, apply access controls, and create an incident-response plan.			

New York CFM Connections: Digital Identity, Cybersecurity, Data Privacy, and Hybrid Collaboration

Cybersecurity is part of every career pathway. Employees protect information by using approved systems, strong authentication, minimum necessary access, secure sharing, verified requests, updated devices, and prompt reporting. A student should not investigate an attack beyond training or hide a mistake.

Term	Student-friendly meaning
Cybersecurity	Protection of systems, accounts, and information from harm or unauthorized access.
Phishing	A deceptive message designed to obtain information or trigger an unsafe action.
Multi-factor authentication	A second verification factor beyond a password.
Least privilege	Giving only the access needed for a role.
Sensitive information	Information requiring protection under law, policy, or responsible practice.
Incident response	Organized actions used to contain, report, investigate, and recover from a security event.
CLASSROOM USE All people, employers, figures, brackets, and documents in this packet are fictional. Never place a real Social Security number, employer ID, bank number, or tax document in classroom work.	

Part 1 - Classify Workplace Information

Sort public event flyer, employee schedule, customer email, password, student record, and de-identified report.

Information	Classification	Who needs access	Safe handling
Event flyer			
Schedule			
Customer email			
Password			
Student record			
De-identified report			

Classification follows policy; de-identification must be checked.

Part 2 - Analyze a Fictional Phishing Message

Message says an account closes in 20 minutes, uses a misspelled domain, requests login, and includes an unexpected attachment.

Signal	Why suspicious	Safe verification	Do not do
Urgency			
Sender/domain			
Login link			
Attachment			
Greeting			
Request			

Do not click or forward the live content.

Part 3 - Apply Access-Control Decisions

A shared project folder contains customer data and is visible to the entire club.

User/role	Access needed	Permission level	Safeguard/review
Project lead			
Data checker			
Designer			
New member			
Former member			
External vendor			

Access is based on role, not friendship or convenience.

Part 4 - Sequence a Security Response

A student clicked a suspicious link and entered a password.

Step	Action	Why	Who/record
1			
2			
3			
4			
5			
6			

Follow the organization’s current procedure; do not erase evidence.

Part 5 - Write a Data-Protection Protocol

Write 150–200 words covering accounts, devices, files, sharing, phishing, and incidents.

Protocol element	Rule/evidence
Passwords/MFA	
Devices	
Storage	
Sharing	
Access review	
Phishing	
Incident report	
Training review	

Never put real passwords or confidential data in the worksheet.