



MADLY PRODUCTIVE PATHWAYS

PROJECT-BASED CTE CURRICULUM
FOR BUSINESS & TECH CLASSROOMS



TERMS OF USE

Thank you for supporting independent curriculum design.

By purchasing this resource, you are agreeing that the contents are the property of Be Madly Productive and licensed to you only for classroom/ personal use as a single user. I retain the copyright and reserve all rights to this product. Please remember to [leave feedback](#) so you will earn TPT credits, which may be applied to your future purchases.

✓ DO:



Use free and purchased items for your own classroom students/personal use.



Reference this product in blog posts, at seminars, PD, workshops, or other such venues. ONLY if both credit is given to myself as the author, AND a link back to my store is included in the presentation.



Purchase licenses at a great discount for other teachers to use this resource.

✗ DON'T:



Claim this work as your own, alter the files in any way, or remove copyright / watermark.



Sell the files or combine them into another unit for sale / free.



Post this for sale / free elsewhere on the internet (including Google Doc links on blogs).



Make copies of purchased items to share with others (violation of the TOU and the law).

≡ STAY CONNECTED! ≡



Follow the Store!

Follow the [store](#) for new resources, sales, and discounts!



Join the Email List

Sign up [HERE](#) for exclusive freebies, teaching tips, and resource updates to your inbox!



Check Out Bundles!

Save time, money, and ENERGY with the full year bundles!



BUSINESS MINDS. TECH SKILLS. ENDLESS POSSIBILITIES.
Preparing students today. Leading tomorrow.



MADLY PRODUCTIVE PATHWAYS

EARN FREE TPT CREDITS!

SUPPORT A TEACHER & SAVE ON FUTURE PURCHASES!

WHAT ARE TPT CREDITS?

TPT credits can be used toward future purchases on Teachers Pay Teachers (like a gift card).

You earn credits by leaving reviews on resources you've purchased.

HOW CAN I EARN THEM?



Leave a review on a resource you purchased.



Earn 1 credit for every \$1 you spend.



Use your credits on ANY future TPT purchases!

⇒ BUILD YOUR CURRICULUM TOOLKIT ⇐

Check out these matching resources to save time and facilitate meaningful learning.

UNIT BUNDLES

Deep-dive instruction organized by unit.



FULL YEAR CURRICULUM

Everything you need for the entire year.



PROJECTS & CASE STUDIES

Real-world projects that build skills.



AP & EXAM PREP

Prepare students to succeed on exams.



JOIN THE EMAIL LIST FOR
EXCLUSIVE FREEBIES AND PROJECT-
BASED TEACHING TIPS!



SCAN TO JOIN

Stay in the loop with new resources, sales, and classroom ideas



PROJECT-BASED. REAL-WORLD. FUTURE-READY.

Topic 1.1: Understanding Social Engineering

LO: 1.1.A, 1.1.B, 1.1.C | Skill: 1.A | Scenario: 1A: Detecting Phishing Messages

Welcome to Topic 1.1

This is the teacher's command-center document for Topic 1.1: Understanding Social Engineering. Read this first before printing or assigning anything.

Topic	1.1 — Understanding Social Engineering
Unit	1: Introduction to Security
Estimated Time	2 class periods (CED recommendation, 45 min each)
Learning Objectives	1.1.A, 1.1.B, 1.1.C
Skill Focus	Skill 1.A
Unit Scenario	1A: Detecting Phishing Messages
Original Case	Westbrook Gear Co. (original fictional scenario — no CB-protected content)
Mini-FRQ (Device Security Analysis format)	Mini Device Security Analysis — 2 sources (email + policy) + Parts A & B (5 pts)
Credential Tie-In	AP Cybersecurity Credential aligned · CompTIA Security+ obj. 5.6 (social engineering)
Teacher Prep	Across 2 days — print Guided Notes, Worksheet, Scenario Brief, Collaboration Activity, Exit Ticket, MCQs, Mini-FRQ. Slides for projection.

What students will know + do by the end

- Identify the two primary psychological tactics (intimidation, urgency) used in social engineering attacks.
- Spot 4-6 concrete red flags in a phishing email or text message.
- Explain how those tactics exploit normal human psychology to bypass critical thinking.
- Describe three categories of impact when a social engineering attack succeeds: personal-info disclosure leading to impersonation, secure-info disclosure (one-time passwords) leading to account takeover, and malware installation or credential capture.

Deliverables (this topic ships 12 files)

Every file is print-ready and audit-verified. Folder paths shown.

File	Where it lives
READ FIRST	00 Start Here / 00_READ_FIRST_Teacher_Guide.pdf
Lesson Plan (2-day)	00 Start Here / 1.1_Lesson_Plan.pdf
Standards Map	00 Start Here / 1.1_Standards_Map.pdf
Slide Deck	01 Present / 1.1_Slides.pptx
Bell Ringer (Day 1)	01 Present / 1.1_Bell_Ringer.pdf
Guided Notes (Student)	02 Student Handouts / 1.1_Guided_Notes_Student.pdf
Vocab Slip	02 Student Handouts / 1.1_Vocab_Slip.pdf
Application Worksheet	02 Student Handouts / 1.1_Worksheet_Student.pdf
Scenario Brief (Student)	03 Scenario / 1.1_Scenario_Westbrook_Gear_Student.pdf
Collaboration Activity	04 Collaboration Activity / 1.1_Collab_Phishing_Triage.pdf
Exit Ticket	05 Assessment / 1.1_Exit_Ticket.pdf
MCQ Practice Set	05 Assessment / 1.1_MCQ_Practice_Set.pdf
Mini-FRQ	05 Assessment / 1.1_Mini_FRQ.pdf
Guided Notes Key	06 Answer Keys / 1.1_Guided_Notes_Key.pdf
Worksheet Key	06 Answer Keys / 1.1_Worksheet_Key.pdf
Scenario Teacher Key	06 Answer Keys / 1.1_Scenario_Westbrook_Gear_Teacher_Key.pdf
Exit Ticket Key	06 Answer Keys / 1.1_Exit_Ticket_Key.pdf
MCQ Key	06 Answer Keys / 1.1_MCQ_Key.pdf
Mini-FRQ Teacher Key	06 Answer Keys / 1.1_Mini_FRQ_Teacher_Key.pdf

Teacher prep checklist

- Print Guided Notes, Worksheet, Scenario Brief, Collaboration Activity, Exit Ticket, MCQs, Mini-FRQ — one per student.
- Project Slides (1.1_Slides.pptx). Verify projector + audio not needed (no embedded media).
- Skim CED pp. 40-41 if helpful — 3 LOs (1.1.A/B/C), 8 EKs, suggested Skill 1.A.
- Decide whether to assign Mini-FRQ in-class (Day 2 closer) or as homework.
- Pre-read the Scenario Teacher Key so you can guide Day 2 debrief without slowing the discussion.

Where this topic fits

Within Unit 1 (Introduction to Security): Topic 1.1 is the door-opener. It establishes that *the easiest path to a breach is often the human*, not the code. Topics 1.2-1.5 build outward from this premise: weak authentication, public-network risks, AI-augmented attacks, and AI defense.

Within the full course: the psychological-tactic vocabulary set up here (intimidation, urgency, elicitation) reappears in Unit 5 application-level attacks. The defender-mindset framing established here is repeated across every unit.

ETHICS REMINDER

AP Cybersecurity is taught from the defender's perspective. Do NOT have students compose phishing messages they would actually send. The Collaboration Activity uses sample phishing emails for analysis only — no live targeting.