Answer Key

Every page in this lesson is keyed. Nothing is left as "answers will vary."

Online game

Tag the Tactic, about 9 to 12 minutes: madlyproductivepathways.com/play/tag-the-tactic

Ask afterward: Which message had no tricks at all, and how could you tell?

When: Use the game in addition to the lesson, as a finish-early task, homework or an extra period. Or use it instead of the paper activity. If the game replaces the paper activity, grade the lesson by its exit ticket.

The game plays in the browser on a computer or tablet, with no account. It is not made for phones.

Bell Ringer — Would You Tap the Link?

Look for

- Names something that makes it feel real or urgent, like the real order or the 12-hour deadline.
- Names checking the order through the store's own app or website.

Model response

He really did order something, and the 12-hour deadline rushes him. He could open the store's app or website himself and check his order there.

Also accept: Any real reason from the text in question 1, and any check Devon starts himself in question 2.

Do not accept: A question 2 answer that taps the link to see if it's real.

When to give the point: Give the point for question 1 for the real order or the rush, and for question 2 for any check Devon starts himself.

Guided Notes

Blanks are shown filled in, in order.

What is social engineering?

Tricking a person into giving up information, access or money, or into doing something that helps the attacker, is **social engineering**.

It's often the first step in breaking into an account or a computer.

A fake message that pretends to come from someone you trust, so you'll click a link, open a file, sign in, pay or share information, is **phishing**.

Where can phishing come from?

Phishing by text message is **smishing**.

Phishing by phone call or voice message is **vishing**. If a message gives you a number to call, calling it can reach the scammer.

Phishing with a QR code is **quishing**. Treat a QR code like a link you can't read yet.

A fake message made for one person or a small group, often using real details about them, is **spear phishing**.

It may use your real name, school, teacher or team, so those details don't prove it's real. A message from a friend's account can be fake too, because accounts get hacked.

What other tricks do scammers use?

Making up a story or pretending to have a role, like a new student or a repair worker, to get someone to share information is **pretexting**.

Offering something, like a free download, a prize or a found USB drive, so someone opens or plugs in something harmful is **baiting**.

It can work on your wish to help, like finding a drive's owner. Don't plug in a drive you found. Give it to an adult or the office.

How do phishing messages get you to act?

A way a message gets you to act before you think is a **persuasion tactic**.

Authority and trust tactics pretend to be someone you'd listen to, like a teacher, a bank or a friend.

Urgency, fear and scarcity tactics rush you or threaten you with a loss.

Curiosity and reward tactics tease something to see or offer something free.

Many scams also tell you to keep it secret or not to call anyone. That's a warning sign too.

Can you tell by how a message is written?

A greeting like Dear Customer or Dear Student that could go to anyone is a **generic greeting**, and it's a warning sign.

AI can fix the spelling and grammar mistakes people used to look for, so good writing proves nothing. Bad writing is still a warning sign.

A real company will give you time to check. No rush doesn't mean it's safe, so check any message that asks for a password, a code, money or a download.

Exit Ticket

1. Correct: (B) Phishing by text message.

Smishing is phishing by text. Vishing is by phone, and quishing uses a QR code.

2. Correct: (A) Scarcity and urgency.

"Only 3 spots left" is scarcity, and "in the next hour" is urgency.

Item 3 — written response

Look for

- Names a tactic the message uses, like curiosity, urgency or fear.
- Says the account could be hacked or faked, so the name isn't proof.

Model response

It uses curiosity, and "before everyone else does" adds urgency. His cousin's account could be hacked, so the name on the message doesn't prove his cousin sent it.

Also accept: Any tactic the message really uses, and any reason the account might not be the cousin's.

Do not accept: An answer that trusts the message because it came from a family member.

Points: give 1 point for each line under Look for, 2 in all.