Identity Isn't Guaranteed
Review Questions
Answer Key

1. What is “phishing”?

   Target answer: Phishing is a tactic that hackers use to gather sensitive information by posing as a trustworthy entity through email/electronic communication. Ideal answers may mention that this tactic usually tries to get you to click on a link or visit a (fake) website, and may describe it as a form of social engineering.

2. Name *two* ways you can avoid becoming a victim of phishing.

   Answers might include:

   Don’t click on links, download files, or open attachments from emails, IMs, or websites if there’s any clue the sender might not be who they say they are.

   Hover over links before you click on them to make sure the URL matches/to make sure it’s actually the URL you already know belongs to that site.

   Go directly to the bank/service/etc.’s website using their app, the URL you already know, or a search engine (instead of clicking).

   Don’t send sensitive information until you have verified the identity of the online persona you’re sending it to….

3. a. Give *three* examples of pieces of personal information that would be valuable to a hacker or identity thief.

   Possible answers might include:

   Personal identifiers like birthdate, address, social security number….

   Financial identifiers like account numbers….

   Online credentials like passwords and email addresses….

b. Pick *one* of the examples you gave in (a) and list *three* potential consequences of a hacker or identity thief getting ahold of that information.

Answers will depend on choice of example, but could include: Drain your bank accounts; buy things with your credit card; hack into online accounts (via password or "security questions"); read through personal email; obtain government documents; open new accounts in your name; send people spam….

4. Name one method you could use to verify the authenticity of...

   a. An individual who contacts you online:

      Possible answers might include:

      Contact the person you think you're engaging with via non-Internet means of communication.

      Ask mutual friends whether the person actually is travelling/needs money/etc.

      Observe the person's behavior and language and compare it to the in-person behavior of whoever they claim to be.

      Test their knowledge of shared information....

   b. A website or app:

      Possible answers might include:

      Navigating to the website using a known URL/bookmark.

      Searching for the name of the website or app using a reputable search engine.

      Searching for the name of the site/app and the word "scam".

      Checking the address bar for the padlock symbol or an HTTPS address....

5. What are *two* (other) methods you can use to decrease your chances of getting hacked?

   Example answers might include:

   Use secure passwords, and different ones for different services.

   Keep important information like credit card numbers and social security numbers private.

   Be wary of anyone asking for identifying information or an account password by phone, email, or instant messages.

   Think about whether an email message may be phishing before clicking on any links.

   Install anti-virus/anti-malware software.…