EDUCATOR'S COPY

Spam

For each scenario, identify if the message is spam and if you should share information with the person. Please write your response to each question in the space provided.

SCENARIO 1: You receive an email from a lawyer informing you that a distant relative has named you as a benefactor to a sum of money. It reads, "To receive the money, please send me your bank account number and routing number, so we can complete the deposit.

This email is most likely spam. Even if they correctly use your relative's name, they may not be who they claim. The sender could have obtained the information about your relation through other means. Sharing your bank account information is always risky and should be done cautiously. Never send your info to someone unless you contacted them first and even then be very careful. For example, it is probably not a good idea to send your info via email since it is unencrypted. That's why many hospitals, lawyers, and banks have special websites for communication with you.

SCENARIO 2: A friend sends you a text, letting you know that they are trying to look up a photo you showed them earlier but they do not have permission to see it. You can't access your computer right now to send them the photo. They respond, "I can log into your account real quick to download the photo — what's your password?"

While this is not spam, you should not share your passwords with other people. Once they have your password, they can possibly lock you out of your account or access other online accounts with the same password. Additionally, if a third party, hacker, or a bystander sees your message, more people could access your account without your knowledge.

SCENARIO 3: You get an email addressed to you from your school, claiming that many student accounts have been hacked. They claim, "We have recently detected that many student accounts have been compromised. We apologize and are working to fix the problem. To reset your account, please respond to this email with your username and password."

It is common practice to not ask users for this information. Even if the sender looks legitimate, you should assume that any email asking for your password is spam.

SCENARIO 4: You receive an email from your bank where you have a legitimate account. The email says that they have been hacked and that you should log in to change your account password as soon as possible and change the passwords on any accounts that share the same password.

The correct course of action is to open up a new browser window and access the site as you would normally access it. A disclosure of this type (that accounts have been hacked) will normally be mentioned on the company or bank's customer portal. Instructions on the portal should be able to be followed safely. As in Scenario 3, no legitimate actor will request account credentials from you in an email.

Meta | My Digital World