Phishing is an email or message sent to someone that typically explains that there is a problem with their account and urging them to login via a link provided in the email to fix their account details. These emails are often from a bank or iTunes or some sort of company that the person does have an account with. The link takes users to a very professional looking website that mimics the official site run by the company, however, when users enter their account information it won’t accept the password or somehow creates an error for the user. However, the information that they have entered has already been copied and can then be used against them. A copy of a ‘phishing’ attempt is attached at the bottom of this lesson plan with identifying information removed.

Some glaring concerns come up right away:

1) The price is different in two different places

2) The price of a movie trilogy should never be $199.00

3) The website provides a disclaimer that states ‘If this wasn’t you, your account has been compromised. Please follow these steps’ and then provides a link to the fake website.

4) Though it looks similar to an official iTunes receipt, there are discrepancies.

5) Spelling mistakes are often an indication that something is wrong (poor English skills mean it’s likely a fake).

Phishing attempts depend on two things. One, the user’s belief that companies would provide this service to protect them, and two, a sense of panic created by seeing that your account has been closed, charged a large amount of money or compromised. People tend to log in quickly to try to stop further damage, when logging in actually causes the damage.

Ways to avoid falling for a phishing attempt:

1) If you don’t have an account with that bank or company, don’t worry. It’s simply a blanket email sent out to a number of users trying to get you to take the bait.

2) If there seems to be a huge problem – look at it with a critical eye. In the case of the iTunes receipt below, match it up to a real receipt you have received and look for information that is the same or different (hint: they should be exactly the same – except for the price and name of the app or movie ordered – and contain the same account information).

3) Never follow the link in the email. Go to the company’s website and log in using your username and password – any suspicious activity will be noted and you can then call customer support yourself. If it is a bank, check for the ‘lock’ symbol that indicates the site is secure before you enter any information.

4) Track your accounts and usage regularly to catch any purchases or transactions that weren’t completed by you.

5) Protect your passwords! Never give out a password over the phone or online unless you made the call yourself or have checked to ensure that the site is legitimate.

Phishing attempts can also be made over the phone by companies who claim to have noted a breach in your account. They will provide some basic information and then ask for an account number or password. These attempts are similar to the above noted email attempts and should be ignored. Tell the representative that you will call the service provider back when you have your information in front of you, look up the company’s customer service call center number and have them check your account. You may also receive emails or phone calls to advise you that you have won something and that you simply need to provide some level of personal information to verify that you are who you say you are.

Be very careful providing information – often these are a ruse to get banking information as well. If it looks too good to be true – it probably is!