**Phishing**

Phishing (pronounced the same as fishing) is defined as trying to get your information under the guise of being a trustworthy source.

(**ask class) How they would try and phish someone**

Below are some common methods used by attackers to phish information

* They might do this by pretending to be someone else like your boss or a company and ask for your username and password.
* They prey on curiosity and urgency often pretending that you have to open an attachment or click and link that could lead to viruses
* Running a fake sign in page for a commonly used online service. The username and password is then saved by the attacker
* They offer something that seems too good to be true in exchange for a seemingly small thing in return

At the end of the day phishing is a method used by hackers and other malicious actors to try and get you to do something that gives away your information. They rely on trickery and your overall lack of awareness to get what they want. But if you pay a bit of attention you can usually spot a phishing attempt. All you have to do is be cautious. Most phishing attempts have tell tale signs that can give them away.

**(ask class) What signs do you think may give away a phishing attempt**

Some common signs of phishing are listed below in no particular order

* Altered website links. Some phishing attempts try to appear as legitimate by buying a website with a similar name to a well known brand. A great way to spot a phishing attempt would to look out for these fake links. Often these fake websites are made to resemble the real thing so you are more likely to try and sign in with your real username and password which they can then steal. Some examples of this kind of link will be listed below
  + www.mircosoft.com instead of www.microsoft.com
  + www.gooogle.com instead of www.google.com
* Similar to fake website links they may also use fake emails that appear similar to the real thing. For example instead of JohnSmith@microsoftsupport.com they may send an email as JohnSmith@rnicrosoft.ru. Again the goal of this is to gain your trust and therefore make you more likely to share your information
* Poor grammar or spelling. Often phishing attacks target a wide net of users rather than one person. As such many of these fake messages are rushed and are poorly proof read. In addition to this quite often phishing emails may use odd words or phrases that you would not normally use. For example if you got an email from your friend calling you “My love” or “Dearest brother” this may be a sign that the email is fake. The same can be said if you receive an email from your teacher saying “I are very humbly happy that you passed your test. Please click this link to win a free iPhone”. Your teacher would never use such strange language so you should treat this message with suspicion.

**What to do if you think you see a phishing message.**

If you think you have identified a phishing email it is very important that you do not open it. Instead you should try and see if you can contact the sender through a different medium. For example if you saw an email from your teacher telling you your homework is overdue and you have to click a link to get an extension be suspicious. Wait until the next day to ask them in person. Phishing preys on urgency and emotions. If you think something is fake treat it as such. It is better to have a false positive than to give away your username and password to an attacker! Once you establish if a phishing attempt is real or not if it is real you should report it. Let your teacher know then they can let the proper people know about the phishing campaign and put a stop to it

**What do do if you think you have been phished**

The first thing to do if you have been phished is know that you are not alone. Lots of people have been tricked by phishing attacks. Rather than feel bad about it you should try and learn from your mistakes and respond in the correct way. Be sure to change whatever credentials the attackers stole from your. If it is credit card information let your parents know so they can call their bank and prevent the attackers from using it. If it is a username and password go into that account and change the password to something else. Make all of the information obtained from the attack useless.

**Some good external sources relating to phishing**

* [https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#~how-phishing-works](https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html" \l "~how-phishing-works)
* https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44
* https://us-cert.cisa.gov/ncas/tips/ST04-014