Phishing Scam Tips

Phishing messages are unfortunately becoming more and more prevalent in the digital age. These emails are meant to trick you into giving up your personal information. Many times, they will pretend to be members of the IT staff, asking you to provide your username or password. Please be aware of these schemes, and follow these tips in order to better protect yourself:

- Check to see if you recognize the person who sent the message. If you don't know them, do not open any links.
- Look to see if the message is directly addressed to you, or if it is a generic message.
- Look for the official Aurora Public Schools IT department watermark on the message at the bottom of the email.
- Hover over the link in the message. The URL will pop up. Many times, the web address is random letters & numbers, or from a different country. This is a clear giveaway that the email is not legit.
- Misspellings or grammatical errors within the message are often warning signs of phishing.
- **NEVER** send your username, password, or other personal information over email, or to a website that you do not trust.

The Aurora Public Schools IT department will never ask you to provide your confidential information via email. If there is a valid reason we need to access your account, we will call you directly and get your permission first.

You are your own best defense against cyber-crime. Please be wary of any messages that seem strange and use your best judgment in order to protect yourself. If you ever have doubts that a message is legitimate, please contact the help desk immediately. Thank you.