**Tips on how to avoid Phishing Emails**

1. Does the email seem out of the ordinary, is it normal to receive emails like this from that sender?

1. Check the senders email address by moving your mouse over the sender’s name (red arrow). A box will pop up with more information on the sender (green box).  Sometimes it will be obvious that it’s a phishing address, like if the address in the box is different from the displayed address in the email, but other times it might look like it comes from someone that you know.



1. While hackers can trick the "From" to give any name they want, if you hover your mouse cursor over the From name, or click on it, in most email services you'll see the actual address pop up after a few seconds.

**Is the link within the email legit?**

1. Check the link destination before clicking it. To do this just move your mouse over the link in the email (red arrow) but don’t click it. You will see what the destination of that link is in the lower left of the window (green box). This will be the same for Chrome, Firefox, and Internet Explorer. **You can see in the picture that the destination is different from what the email is telling me.**



1. You could also **right-click** on the link, copy it and then paste it into a text document to see where it would really send you.

**Real phishing email example**

I checked it out and didn't reply to it because it has some warning signs of being a phishing email (Gmail also flagged it as spam so that made it more obvious).

1. I have never gotten an email like this from help desk before.
2. The email address of the sender (red arrow) is not the correct address for this kind of email.
3. It’s asking for my network user name and password (green box) which is a classic phishing technique.



