Security

Phishing Emails

If you know you did not buy a couple of 75" Samsung Neo 4K Smart TVs, why are you calling "Best Buy"??? Oh, that's right, you received an email that says you ordered them and to call their "number" if you need to talk to their "Best Buy Customer Service". Do not fall for it! It could have been an Amazon email or text message… Phishing is still the top attacking vector used for stealing your login credentials, banking info, both personal and company data, and more! Here are a few tips to stay safe:

- Did you expect to receive the email?
- Do you know the sender?
- Did you verify the complete email address of the sender?
- Does the email's tone invoke Urgency, Fear, Immediate Action Required?
- Legit companies will not request sensitive information via email.
- Did the email address you by name or just a generic greeting such as "Dear Sir/Ma'am"?
- Do not click on suspicious email links or open suspicious attachments.
- Hover over the link with your mouse cursor to help verify the validity of the link.
- Look out for misspellings, bad grammar, bad syntax.
- Use the Phish Alert Button (PAB) to report your suspicious email.
- Stop! And Think Before You Click!

For any questions or concerns regarding this information, please contact the Collin College Technical Support HelpDesk:

Students:

972.377.1777
studenthelpdesk@collin.edu

Employees:

972.548.6555
helpdesk@collin.edu