Don't Get Hooked!

Why Should I Care?
You are a phishing target at work and at home. You and your information are worth a lot of money to cyber criminals. They will do anything they can to get money. YOU are the most effective way to stop phishing. If you identify a suspicious email, or you are concerned you might be a victim, contact the TSC immediately.

Phishing Indicators
A Check the email address. If it is from a legitimate sender, but the “FROM” address is a personal account, like @gmail.com or @hotmail.com, this is probably an attack. Also, check the “TO” and the “CC” fields. Is the email being sent to people you do not know?

B Be suspicious of emails addressed to “Dear Customer” or other generic greetings. If a trusted organization needs to contact you, they will know your name and information. Also ask yourself: am I expecting an email from this company?

C Be suspicious of grammar or spelling mistakes; most businesses proofread their messages carefully before sending them.

D Be suspicious of messages that require “immediate action” or create a sense of urgency. This is a common technique to rush people into making a mistake. Legitimate organizations will not ask you for your personal information.

E Be careful with links, and only click on those that you are expecting.

F Be suspicious of attachments. Only click on those you are expecting.

G Be suspicious of any message that sounds too good to be true. (No, you did not just win the lottery or get hired for a job you did not apply for!)

H Just because you got an email from your friend does not mean they sent it. Your friend’s computer may have been infected or their account may be compromised. If you get a suspicious email from a trusted friend or colleague, call them on the phone.

Report any Suspicious Email to STOP-SPOOFING@indstate.edu.

For more information about this and other Security Tips, visit our Knowledge Base at indstate.teamdynamix.com/TDClient/KB/?CategoryID=6300

If you believe that you might have revealed sensitive information about your ISU account, such as your password, then please reset your password immediately at isuportal.indstate.edu and contact the ISU OIT Help Desk at 812-237-2910.