WHAT IS SPEAR PHISHING?

What are the risks?

- System or data compromise
- Identity theft
- Financial loss
- Impact to public reputation
- Regulatory fines
- Loss of employee morale

Phishing typically involves a threat actor* attempting to persuade their victims to perform an action (clicking a link, providing sensitive information, etc.) by posing as a reputable company or person through email, text, or over the phone. Spear phishing works the same way, but instead of casting a wide net across an entire organization, threat actors will spend time gathering information to personalize their attack and target a specific individual or department.

**per NIST.gov - an individual or group posing a threat*

Prevention Tips:

Limit Publicly Accessible Information

Threat actors build a 'profile' of their targets using public contact and social network information to make their attacks more believable. Follow data privacy best practices and limit who can view your personal and work information, both on your organization's website and on social media.

Take Your Time!

Phishing attacks are over 50% more successful when the target is distracted. To leverage this, threat actors will make their requests sound urgent (i.e. "I'm in a meeting but I need you to send me this document immediately"). Slow down and always think twice before taking any action.

Verify, verify, verify!

Public directories make it easy for threat actors to impersonate coworkers, bosses, and executives. If you get an unexpected email, message or phone call that prompts you to take an action, contact the supposed sender using a different communication channel to confirm the request is legitimate.

Report Suspicious Activity

Threat actors know if they're smart social engineers, they can fly under the radar and acquire data from unsuspecting employees without ever being detected. If something seems unusual, don't wait! Report anything you find suspicious to **abuse@rutgers.edu** immediately.

Don't get hooked! Always stay informed regarding current scams and social engineering tactics.

RUTGERS

Contact the OIT-Information Security Office:

Web: it.rutgers.edu/information-security **Email: info_security@oit.rutgers.edu**