NYU | Financial Operations and Treasury

CYBER FRAUD PREVENTION

PHISHING

- ***Do not open unknown file attachments or click links in suspicious emails, phone calls, or texts***
- ***Be on lookout for:***
  - *any requests for* ***personal information***
  - *messages about* ***system or security updates, e.g. SSNs or direct deposit banking information***
  - ***urgent appeals*** *claiming your account will be closed if you fail to respond*

REPORT SUSPICIOUS ACTIVITY

TO YOUR SUPERVISOR OR NYU IT IMMEDIATELY

IMPERSONATION

- ***Do not use shared user names or passwords*** *and avoid using automatic login features that save usernames and passwords. Do not use your passwords for other non-related websites that you access*
- ***Call to validate*** *every new or changed beneficiary information payment request received*
- ***Be extra vigilant during holiday or vacation periods*** *when fraudsters try to take advantage of the absence of personnel*
- ***Be suspicious of out of the ordinary urgent requests from NYU leadership*** *for payments or payment information. They will not ask you to transfer funds*

DOWNLOADS

- **Use caution when visiting websites.** *Access only trusted websites for business purposes. Clicking on a document, ad or video, even on a legitimate site, may result in downloading malware*
- ***Be attentive during online session:*** *Are login prompts normal? Do your online screens look correct? Typos and other errors are often the mark of fraudulent emails or websites*
- ***Do not delay updates to your computer.*** *To ensure that system updates are installed,* ***restart your computer daily*** *and periodically completely shut-down your computer*

If it looks 'suspect', report it. Better safe than sorry.

- *Forward emails to phishing@nyu.edu to make NYU IT aware of the phishing attempt*
- *Email security@nyu.edu if you see any content that appears suspicious or unauthorized on an NYU website*

iLearn: TEC 107: Tech Savvy-NYU Individual Information Security