Stony Brook University

Security & Safety Bulletin for Researchers

Bulletin 03 | Research Security Resiliency Team

Research Security & Safety

The Stony Brook University community has many valuable resources to protect. These bulletins are meant to provide quick facts, best practices, and key University contacts.

Phishing / Cyber Hygiene

What is Phishing?

Phishing is a type of cyber-attack where attackers disguise themselves as trustworthy entities to trick individuals into providing sensitive information, such as login credentials or financial information.

Tips for Staying Safe

- Be cautious with emails and communications from unknown sources, especially those that request personal information or urge immediate action, such as logging in with your NetID.
- Do not click on suspicious links or download attachments from unknown or untrusted sources.
- Use a password manager to help create unique passwords for all websites/services (LastPass is offered for free to employees and students)
- Use two-factor authentication where possible to add an extra layer of security to your accounts, including your personal accounts.

Whom to Contact

Forward Suspicious E-Mails to:

phishbowl@stonybrook.edu

Suspicious DUO Prompt:

Change password and open Ticket at https://help.stonybrook.edu

All Other Questions or Concerns:

http://service.stonybrook.edu

More Info:

LastPass

Secure Computing

Date Published: 8/22/2024 Date of last revision: 8/22/2024