

Phishing: Best Practices

- Be suspicious by default
- Scrutinize URLs: verify link targets
- Don't visit sites via links – use bookmarks and keywords or type in the URL
- If you do, check the address in the URL field
- Disclose email address only when necessary
 - Plussing, SPAM filters
- Don't be put at ease by language that suggests a concern for your security
- Maintain a pop-up blocker
- If you provide credentials, you will usually be directed to a secure site (httpS)
- Know common formats of fraudulent links

Passwords: Best Practices

- Do not share your password with ANYONE
- Use different passwords for different accounts and services
- Use complex passwords, letters, numbers, characters, upper/lower case
- Change passwords periodically
- Understand that your PSUID password allows anyone to:
 - Add and drop classes (students)
 - Change benefits (faculty and staff)
 - See where you live
 - View your payroll information
 - Change deductions, auto-deposits
 - View and send email via the web
 - Access Portal and Pass space
 - Edit Grant Proposals (faculty & staff)
 - Modify content on ePortfolio and personal web

SPAM: Best Practices

- Don't supply email address when subscribing to services if it isn't required
- If it is required use a "Plussed" address (supported by PSU accounts)
- Setup and maintain filters
- Don't "unsubscribe" – only confirms your address as valid
- Don't click on links from SPAM
 - Can put you on more mailing lists
 - Can infect your computer with viruses and worms
- NEVER open attachments
 - These are almost always viruses, worms, or Trojan horses