Phishing
Phishing is a form of email fraud where scammers use email messages that appear to come from a legitimate company or institution, such as your bank or university, and they ask you to “update” or “verify” your personal information. Do not provide your social security number, passwords, or confidential personal information in response to an email request. For more info see: What are phishing scams and how can I avoid them?

Password Guidelines & System Practices

This handout covers the following data security topics:
⇒ Password Guidelines
⇒ System Best Practices
⇒ Phishing

Password/Passphrase Guidelines

- Use strong passwords; include combinations of lower and uppercase letters, numbers, and symbols. The longer your password, the better.
- Do not write your username and password or passphrase in the same place.
- Never share your password or passphrase with anyone.
- Never send anyone your password or passphrase via email, even if the message requesting your password seems official. A request for a password or passphrase is very likely a phishing scam.
- Change your password or passphrase every six months.

System Best Practices

- When you leave for the day, please make sure to select the Windows Restart or Logoff options rather than locking your system. It is important that all Windows updates are being applied as scheduled and logging off or restarting your system allows for these updates to be applied.
- If you leave your office for a meeting, please make sure to lock your system as this ensures no one accesses any sensitive student data while you are away.
- If you encounter any errors related to Windows Updates or receive any messages related to viruses, please make sure to contact your LSP.
- Do NOT install any applications that have not been approved by the department.