INFORMATION SECURITY FOR ASU FACULTY

Information Security is a shared responsibility and each of us has a role to play. It is important to remember that good information security practices not only protect the University’s data but also our own personal data and reputation.

What Do We Need To Do?

- **Be Aware of What Constitutes “Confidential Information”** - The University is legally, contractually, and ethically obligated to protect a variety of information related to students and employees. “Confidential” data relates to any information whose loss or exposure may result in financial and reputation issues for the institution (see sidebar for examples). **When dealing (or planning to deal) with confidential data, it is best to reach out to the ITS Office of Information Security for help in determining what security measures may be needed.**

- **Beware of Scams Like Phishing** - Employ a healthy degree of skepticism with any electronic message or phone calls that ask you to visit a website and provide your password or other personal information. These attempts can look very realistic but always remember that ITS will never ask you for your username and password!

- **Keep Your Computer Up To Date** - When we are busy, it is often hard to find time to update your computer; However these updates often contain security fixes that keep you safe from a variety of hacking attempts. A good practice is to install these updates at the end of the day before leaving.

- **Lock Your Computer When You Step Away** - When you leave your computer for a prolonged period, it is advisable to lock your screen to prevent others from viewing information or accessing any accounts you may have logged into. Also make sure to logout of any public campus computers (labs, podium systems) when you are done with them.

- **Report Issues Promptly** - If you note something suspicious or believe you may have been a victim of a cyber scam or attack, the best thing is to report this right away by calling the ITS HelpDesk at 828-262-6266.

How Can I Get Help?
The ITS Office of Information Security is here to help the Appalachian Community with Information Security issues and concerns. We can be reached at:

<table>
<thead>
<tr>
<th>Phone: 828-262-6946</th>
<th>Email: <a href="mailto:security@appstate.edu">security@appstate.edu</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Fax: 828-262-2236</td>
<td>Web: <a href="http://security.appstate.edu">http://security.appstate.edu</a></td>
</tr>
<tr>
<td></td>
<td>Twitter: <a href="https://twitter.com/appinfosec">https://twitter.com/appinfosec</a></td>
</tr>
</tbody>
</table>

Security Tips and Resources

**Examples of Confidential Data**
- Social Security Numbers
- Employer Tax ID Numbers
- Drivers License Numbers
- Passport Numbers
- State Identification Card Numbers
- Check / Savings Acct. Numbers
- Credit or Debit Card Numbers
- Personal Identification (PIN) Code
- Electronic Identification Numbers
- Passwords
- Biometric Data
- Digital Signatures
- Privately-Owned Trade Secrets
- Private Contributor Records
- Human Subject Research Data
- Medical Records (PHI)
- Disability Records
- Data Protected by Non-Disclosure Agreements
- Criminal Investigation Records

**Use ASU Filelocker To Securely Exchange Files**

Filelocker

If your work requires that you transmit information that might be confidential or sensitive then don’t use email to send files. Use ASU Filelocker!

http://filelocker.appstate.edu

**Quick Tip: Lock Your Screen**

If you use a Windows computer you can lock your screen with two simple-keys.

To set up a quick screen-lock shortcut on Mac see here:

http://goo.gl/1Dfwy9

**Home PC Security Checkup**

Did you know that Faculty members can take their home PCs to the ITS Technology Support Center for free assistance with virus removal and security review.

Phone: 828-262-6266