Security Awareness Tools and Resources

Remote Access Tools

Data Encryption

Data encryption is a method that can allow you to safeguard electronic information by preventing unauthorized access to files. Encryption software converts "plain text" data that can easily be read into encrypted data via complex mathematical operations and a unique key. Encryption keys work similarly to physical keys to doors or a locked filing cabinet. Without the key, gaining access to encrypted data is often extremely difficult. Most often encryption keys take the form of passphrases where only individuals who have the passphrase can decrypt and view the data.
Access to encrypted data is dependent on your key (see above), making it possible that if you lose your key you may lose access to your data. It is very important to consider how you might securely back up and protect your encryption key when considering encryption.
Most often when a computing device is lost or stolen, the data on the device is unencrypted and therefore easy to access (even if the device is password protected). However, using encryption protects sensitive data and keeps it private.

Another common use of encryption is in creating encrypted containers (more below) so that even if a computer is infected with malware there is an additional layer of protection that may thwart intruders from accessing confidential or sensitive data.
Full Disk Encryption is used to safeguard all data stored on a hard drive (including the operating system).

File Level Encryption uses a single key or multiple keys to encrypt a single file or series of files only.

Container-Based Encryption provides encryption of a container file that internally contains other files that can be read (i.e. encrypted zip file).
Full Disk Encryption is used to safeguard all data stored on a hard drive (including the operating system).

File Level Encryption uses a single key or multiple keys to encrypt a single file or series of files only.

Container-Based Encryption provides encryption of a container file that internally contains other files that can be read (i.e. encrypted zip file).

- Encrypting Android Devices
- Verify iOS Device Encryption
- Encrypting Windows PC *Note: Enterprise + Ult. Editions Only*
- Encrypting Windows 8 PC *Note: Pro + Ent. Editions Only*
- Encrypting Mac Systems using File Vault

Creating and Managing Passwords

Your data encryption protection is only as secure as your encryption key. Use App State's Tips for Creating a Secure Password. Also, consider using a password manager tool such as KeePass which securely stores passwords.

Antivirus

- Windows Secunia PSI - *Free Tool To Keep Your PC Patched*
- Mac OS/X Sophos Free Antivirus For Mac
- DNS Service Malware Protection
- Visit support.appstate.edu/students for free antivirus software, and other support information for students

- Protect yourself and App State data from phishing threats with our Internal Phishing Testing
- Have you been a victim of phishing? Read our Phishing Victim Advisement
- Protect yourself from common information security threats by viewing our Google Slides

Additional Secure Tools

- Secure File Exchange (FileShare)
- Duo Two-Factor Authentication Enrollment for Faculty & Staff

Security Awareness Resources

- KnowBe4 Security Awareness Training for Faculty & Staff
- View OUCH! Monthly Security Awareness Newsletters
- Learn to identify Common Security Threats

Related Articles

- Common Security Threats
- How to Update my Appstate Password
- Mobile Device Security Guidelines
- Security
- Security and Google Apps
- Security Awareness

- Security Awareness Training
- Unlocking Bitlocker-Locked Computer

We value your feedback! Click HERE to suggest updates to an existing article, request a new article, or submit an idea.

Search Knowledge Base

Submit a Service Request