



**Missouri State**<sup>™</sup>  
U N I V E R S I T Y

# **Ensuring Customer Security and Privacy within Your Web Site**

Web Developers Users' Group

April 22, 2008

# Why?

- **To give your customers the safest, best browsing experience on your web site**
- **To stop hackers, spammers and other “bad people”**
- **To save the University from bad publicity**



# What needs to be secure?

- Passwords
- Credit card numbers
- Social security numbers
- Personally identifiable data
- Anything you don't want the public to know



# Credit Card Numbers

- **Should never be handled by unit or organization online forms**
- **If online, must be processed by central credit card processing service**



# How?

- **Permission**
- **Password protection**
- **Encryption**
- **Correct form submission method**
- **Proper coding**

# Permission

- **Don't post anything that you don't have permission to publish**
  - [Image, voice or likeness](#)
  - [Intellectual property](#)
  - [Personally identifiable information](#)

# Password Protection

- Prevents search engines and others from being able to access your content without logging in
  - [Single Sign On](#) ([example](#))
  - [Restricted web sites](#) ([example](#))

# Encryption

- **Secure web sites encrypt all data sent to or received from it**
- **Helps prevent people from intercepting data during transmission**
- **Address begins with *https://***
- **[Learn more](#)**



# Correct Form Submission Method

- Do not request that confidential information such as social security, credit/debit card, or bank account numbers be returned by email
- Use database forms instead of email forms



# Proper Coding

- [Open Web Application Security Project](#)
- [.NET Security](#)
- [ASP Security Issues](#)
- [PHP Top 5](#)